SMJERNICE
ZA UČINKOVITU PRIMJENU OPĆE UREDBE O ZAŠTITI PODATAKA

(Uredba (EU) 2016/679)

Priručnik namijenjen službenicima za zaštitu podataka u javnom sektoru

Priređeno u okviru T4DATA (2014-2020) programa, financiranog iz fonda Europske unije.

Ugovor o bespovratnim sredstvima broj: 769100-T4DATA—REC-DATA-2016/REC-DATA2016-01)

I. IZDANJE

Sufinancirano kroz Program o pravima, jednakosti i građanstvu Europske unije (2014 – 2020)

autori:

Douwe Korff, Marie Georges i članovi Grupe the Fundamental Rights Experts Europe (FREE) uz veliki doprinos hrvatskog tijela za zaštitu osobnih podataka i partnera projekta.

Priručnik za službenike za zaštitu podataka
(SZP-ove)

Smjernice za službenike za zaštitu podataka u javnom i gotovo isključivo-javnom sektoru o tome kako osigurati usklađenost s Općom uredbom o zaštiti podataka Europske unije

(Uredba (EU) 2016/679)

Izrađeno za "T4DATA" projekt financiran iz fondova EU

(Ugovor o bespovratnim sredstvima broj:
769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

[1. izdanje – u obliku podnesenom Europskoj komisiji]

PRVI SVEZAK:
Glavni dio teksta

autora

Douwe Korff

Profesor emeritus Međunarodnog prava,
the London Metropolitan University
Izvanredni profesor, Oxford Martin School, University of Oxford

i

Marie Georges

Neovisni međunarodni stručnjak za zaštitu podataka
(ex-CNIL, EU, Vijeće Europe itd.)

Članovi Grupe the Fundamental Rights Experts Europe (FREE)

Na temelju značajnog doprinosa talijanskog tijela za zaštitu osobnih podataka i partnera projekta

(Po odobrenju Komisije, srpanj 2019.)

O ovom Priručniku:

Ovaj je Priručnik izrađen kao dio materijala za edukaciju u okviru "T4DATA" projekta financiranog iz EU fondova u svrhu edukacije edukatora (*training of trainers*). Priručnik je namijenjen osposobljavanju zaposlenika u tijelima za zaštitu osobnih podataka u državama članicama Europske unije s ciljem edukacije službenika za zaštitu podataka, posebice u javnom sektoru, u vezi njihovih obveza iz Opće uredbe o zaštiti podataka (Uredba 2016/679, GDPR). Projekt je implementiran pod okriljem talijanskog tijela za zaštitu osobnih podataka, *Garante per la protezione dei dati personali,* a koordinator projekta je zaklada *Fondazione Basso*. Veliki doprinos projektu dali su stručnjaci iz Grupe *the Fundamental Rights Experts Europe* (FREE), gđa Marie Georges i prof. Douwe Korff.

Priručnik je nastao temeljem zajedničkog doprinosa **talijanskog nadzornog tijela za zaštitu podataka *Garante per la protezione dei dati personali* i hrvatskog nadzornog tijela za zaštitu podataka-Agencije za zaštitu osobnih podataka** te drugih tijela za zaštitu podataka, partnera u ovom projektu, koji su doprinijeli ovom priručniku s vrlo korisnim i praktičnim primjerima i smjernicama za implementaciju GDPR-a.

Naglašavamo da u slučajevima kad se tekst u priručniku referira na neki od prethodnih radova gđe Georges i prof. Korffa, njezino/njegovo ime se nalazi u povezanoj bilješci (fusnoti) samo u slučajevima kad se radi o javno dostupnim resursima. To je rijetko u slučaju Marie Georges, uglavnom zbog institucionalnih ili povjerljivih razloga vezanih uz njezin rad na zaštiti podataka za nacionalna i međunarodna vladina tijela.

Za više informacija o ovom projektu, partnerima i stručnjacima, pogledajte: https://azop.hr/t4data/.

Iako je priručnik izrađen u okviru "T4DATA" projekta, **može biti koristan i svima onima koji su zainteresirani za primjenu GDPR-a, a posebno službenicima za zaštitu podataka (u javnom ili privatnom sektoru).** Javno je dostupan pod licencom "Creative Commons" (CC).

Bilješka: S obzirom da ovaj priručnik također ima namjeru podržati obuku službenika za zaštitu osobnih podataka (SZP-ova) u obavljanju njihovih obveza na temelju GDPR-a, isti se fokusira na europsko pravo zaštite osobnih podataka, a podrobnije na pravo zaštite osobnih podataka vezano za ono što se ranije nazivalo predmetima iz "prvog stupa" ili "pitanja unutarnjeg tržišta". Međutim, odlomci 1.3.4 – 1.3.6 i 1.4.3 – 1.4.5 još uvijek sadrže pravila i instrumente zaštite podataka koji su se primjenjivali ili se primjenjuju na ostala pitanja obuhvaćena pravom Europske unije, odnosno pitanja koja su bila obuhvaćena područjem "pravosuđe i unutarnji poslovi" [PUP], odnosno trećim stupom, a danas je to područje "sloboda, sigurnost i pravosuđe" [SSP]. Predmetno područje odnosi se na tzv. zajedničku vanjsku i sigurnosnu politiku [ZVSP] – prethodno poznatu kao drugi stup te na aktivnosti europskih institucija općenito. Pododlomak 1.4.6 odnosi se na prijenos podataka između različitih europskih sustava. Također nije obuhvaćena zaštita podataka izvan područja EU/EGP, iako smatramo da bi SZP-ovi trebali steći barem neki stupanj znanja o glavnim utjecajima koje su imala EU pravila, a i dalje ih imaju, na zaštitu podataka diljem svijeta. Nadamo se da ćemo biti u mogućnosti dodati ta područja u kasnijim, revidiranim verzijama ovog priručnika, u kojima ćemo tada također biti u mogućnosti ažurirati informacije o pitanjima koja ostanu otvorena u vrijeme pisanja ovog prvog izdanja, kao što su, posebice, razvoj Uredbe o e-privatnosti, koja je u vrijeme pisanja ovog priručnika i dalje u ranim fazama zakonodavnog procesa.

Priručnik je također dostupan na talijanskom, hrvatskom, bugarskom, poljskom te španjolskom jeziku, odnosno službenim jezicima svih zemalja partnera ovog projekta.

IZJAVA O ODRICANJU ODGOVORNOSTI:

Informacije i stavovi sadržani u ovom priručniku pripadaju isključivo autorima i kao takvi ne predstavljaju nužno službeni stav Europske unije. Institucije Europske unije, kao ni osobe koje djeluju u njihovo ime, nisu odgovorni za upotrebu informacija koje se nalaze u ovom priručniku.

SADRŽAJ

Nastavak sadržaja:

MJERNICE ZA SLUŽBENIKE ZA ZAŠTITU OSOBNIH PODATAKA O TOME KAKO OSIGURATI USKLAĐENOST S EUROPSKOM UREDBOM O ZAŠTITI PODATAKA

(Uredba (EU) 2016/679)

UVOD

25. svibnja 2018. godine u primjenu je stupila nova europska Opća uredba o zaštiti podataka (**GDPR** ili "**Uredba**")[1], zamjenjujući Direktivu o zaštiti podataka iz 1995. godine ("Direktiva iz 1995").[2] Usvojena kao odgovor na masovno širenje obrade osobnih podataka od uvođenja Direktive iz 1995. godine, kao i odgovor na razvoj sve invazivnijih tehnologija, Uredba se temelji na Direktivi, kao i sudskoj praksi Suda Europske unije (SEU) razvijenoj na temelju te Direktive. U tome ona ima značajno veći doseg od Direktive i pri tome značajno ojačava glavni europski sustav zaštite podataka. Ona donosi mnoge promjene u smislu mnogo većeg usklađivanja, jačih prava ispitanika, bolje prekogranične suradnje u provedbi između nacionalnih tijela za zaštitu podataka (TZP-ovi) itd.

Među najvažnije promjene ubrajaju se uvođenje novog načela "odgovornosti [pouzdanosti]" i institucije službenika za zaštitu podataka (**SZP-ova**), koje imenuje voditelj obrade podataka. Ovo je dvoje povezano: SZP-ovi su osobe koje će u praksi morati osigurati usklađenost s načelom odgovornosti/pouzdanosti od strane i unutar organizacija kojima pripadaju. Ovaj Priručnik ima svrhu podržati nove SZP-ove iz javnog sektora u tom nastojanju.

1 Puni naziv: DIREKTIVA 95/46/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281 od 23.11.1995. g., dostupna na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:31995L0046&from=en
Napominjemo, iako je Uredba donesena 2016. te stupila na snagu dvadesetog dana od objave u Službenom listu Europske unije tj. 25. svibnja (čl. 99. st. 1.), ona je ušla u primjenu, odnosno izravno se primjenjuje u svim državama članicama od 25. svibnja 2018. godine (čl. 99. st. 2.)

2 Puni naziv: DIREKTIVA 95/46/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281 od 23.11.1995.g., dostupna na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:31995L0046&from=en.

Priručnik se sastoji od tri dijela:

- **Prvi dio** predstavlja pojmove "povjerljivosti", "privatnosti" i "zaštite podataka" te prve zakone koji se tiču zaštite podataka - načela i međunarodne instrumente (posebice Konvenciju Vijeća Europe o zaštiti podataka iz 1981. godine), prije rasprave o europskim direktivama o zaštiti podataka iz "prvog stupa" iz 1990-ih i ranih 2000-ih te uvođenje nedavno usvojenih i predstojećih budućih instrumenata o zaštiti osobnih podataka (GDPR, predložena Uredba o e-privatnosti, te "modernizirana" Konvencija Vijeća Europe);[3] Prvi dio još uvijek ne raspravlja o instrumentima EU-a iz "trećeg stupa" iz 1990-ih i pravilima o zaštiti podataka za vlastite institucije EU-a i njihove nasljednike.

  * Nadamo se da će se u budućnosti moći izdati prošireno, drugo izdanje ovog priručnika koje će ispravno obuhvatiti te instrumente.

- **Drugi dio** pruža pregled svih ključnih elemenata Opće uredbe o zaštiti podataka, prije fokusiranja na dodatno, novo temeljno načelo "pouzdanosti"/ ["odgovornosti"] i koncepata te pravila iz GDPR-a koja se odnose na Službenika za zaštitu podataka; i
- **Treći dio** pruža praktične smjernice o tome kako SZP-ovi u javnom sektoru mogu i trebaju ispunjavati svoje brojne zadaće, sa stvarnim primjerima iz života, posebice onima koji se odnose na tri glavna područja: obrazovanje, financije i zdravstvena njega, te vježbe.

Pored opširnih referenci i poveznica na materijale u bilješkama (fusnotama), odvojeni drugi svezak uz priručnik sadrži opširne daljnje materijale koji su dostupni sudionicima na edukacijama u okviru "T4DATA" projekta.

Internetske (mrežne) stranice:

Što je moguće više gore navedenih materijala i internetskih poveznica bit će također dostupno na javno dostupnim mrežnim stranicama koje su navedene u ovom Priručniku (Priručnik je dostupan za slobodnu i besplatnu uporabu temeljem "*Creative Commons*" licence http://www.fondazionebasso.it/2015/t4data-training-data-protection-authorities-and-dataprotection-officers/).

3 [3] O ograničenjima koja se tiču dotičnih pitanja, vidjeti Bilješku u djelu "*O ovom priručniku*".

PRVI DIO
Podrijetlo i značenje zaštite podataka

U ovom se dijelu nastoji objasniti što je to zaštita podataka i kako se razvijala u Europi te na koji način novi i "modernizirani" europski instrumenti o zaštiti podataka pokušavaju odgovoriti na najnoviji tehnološki razvoj.

- Odlomak 1.1 raspravlja o raznolikim (ako se preklapaju) konceptima povjerljivosti, privatnosti i privatnog života te zaštiti podataka i pristupu potonjem kako se isti razvijao u Europi, uključujući i zahtjeve iz područja ljudskih prava i vladavine prava u Europi koji su temelj zaštite podataka.
- Odlomak 1.2 obuhvaća podrijetlo zaštite podataka u Europi, pojavu osnovnih načela zaštite podataka i prava koja iz toga proistječu te njihov razvoj u europskim i globalnim neobvezujućim pravnim instrumentima (aktima) – te jedan obvezujući, Konvenciju Vijeća Europe o zaštiti podataka iz 1981. (uključujući njen Dodatni protokol).
- Odlomak 1.3 bavi se načinom na kojemu su se dalje razvijala pravila i načela zaštite podataka u Direktivama EZ-a o zaštiti podataka iz 1990-ih i 2000-ih (kako bi se omogućio razvoj "unutarnjeg tržišta" EU-a, koji je bio potreban i slobodan protok podataka te zaštita temeljnih prava na zaštitu podataka), s fokusom na Direktivu o zaštiti podataka 1995. (čime je 2001. godine Dodatni protokol uz Konvenciju iz 1981. težio uskladiti tu Konvenciju; pododlomak 1.3.1 i 1.3.2.) te govori o posebnim pravilima primjenjivim u telekomunikacijskom sektoru (pododlomak 1.3.3).

  Posljednji pododlomak ovog odlomka sadrži instrumente zaštite osobnih podataka unutar nekadašnjeg područja "pravosuđa i unutarnjih poslova" [PUP] (pododlomak 1.3.4), u vezi sa zajedničkom vanjskom i sigurnosnom politikom [ZVSP] (pododlomak 1.3.4) te za institucije EU općenito (pododlomak 1.3.6).
- Odlomak 1.4 uvodi najnovije pravne instrumente, usvojene kako bi se išlo ukorak s budućnosti: europska Opća uredba o zaštiti podataka iz 2016. godine (GDPR, u primjeni od 25. svibnja 2018. g. (pododlomak 1.4.1)) te predlaže zamjenu Direktive EZ o e-privatnosti iz 2002. g. novom Uredbom o e-privatnosti; (pododlomak 1.4.2).

  Sljedeći pododlomak u ovom odlomku ukratko bilježi ključne nove instrumente unutar sadašnjeg područja "pravosuđe, sloboda i sigurnost" [JFS], provedbu Direktive o zaštiti podataka iz 2016 (pododlomak 1.4.2); položaj u odnosu na ZVSP (pododlomak 1.4.4) te novosti koje se odnose na instrumente za zaštitu podataka institucija EU, Regulativa 2018/1725 (pododlomak 1.4.5). Pododlomak 1.4.6 razmatra protok podataka između različitih europskih sustava zaštite podataka.

  "Modernizirana" Konvencija Vijeća Europe, otvorena za potpisivanje u listopadu 2018. godine, razmatra se u posljednjem pododlomku (pododlomak 1.4.7).

  NB: Nadamo se da ćemo predstaviti instrumente zaštite podataka EU-a za gore spomenuta područja (provedbu zakona i pravosudnu suradnju, CSFP te institucije EU-a), usvojene kako bi zamijenile one iz 1990-ih i ranih 2000-ih te najnovija globalna pravila, detaljizirana u drugom izdanju.

GDPR, koji je u samoj srži ovog priručnika, dalje se propituje u drugom dijelu.

1.1 POVJERLJIVOST, PRIVATNOST I ZAŠTITA PODATAKA: RAZLIČITI, ALI KOMPLEMENTARNI KONCEPTI U DOBA DIGITALIZACIJE

1.1.1 Povjerljivost i privatnost

Oduvijek su postojala područja u kojima su privatne informacije tretirane na način da podliježu posebnim pravilima **povjerljivosti**. Tipični primjeri su Hipokratova zakletva iz 4. st. pr. n. e. za **doktore medicine[4],** te rimokatolička "**ispovjedna tajna**".[5] U novije doba, posebice od 19. stoljeća, traži se od **bankara, odvjetnika**, drugih **vjerskih službenika**, **radnika u sektoru pošte i telekomunikacija** i mnogih drugih, da tretiraju informacije koje dobiju od pojedinaca u svojem službenom svojstvu kao povjerljive, privilegirane[6] ili čak kao svetinju.

Općenito se smatra da takve obveze čuvanja povjerljivosti služe ujedno i pojedincu i društvu: pojedinac može imati povjerenje da će osoba kojoj otkriva informacije tretirati iste kao povjerljive, a takvo povjerenje zauzvrat služi javnom dobru, u smislu da odsustvo istoga može odvratiti osobe od toga da traže pomoć ili otkrivaju informacije vlastima, čime se podriva javno zdravlje i druge socijalne koristi, npr. pokušaji da se spriječi širenje spolno prenosivih bolesti ili pak politički ili religijski ekstremizam.

Međutim, kako objašnjava g. Frits Hondius, zamjenik direktora za ljudska prava u Vijeću Europe i ujedno nadležan za izradu prvog međunarodnog obvezujućeg instrumenta o zaštiti podataka, konkretno Konvencije o zaštiti podataka vijeća Europe iz 1981. godine, o čemu se govori u točki 1.2.3 dalje u tekstu), premda je postojala ova obveza čuvanja povjerljivosti u okviru njihovih obveza:[7] nije postojalo odgovarajuće pravo koje bi imali pacijenti, klijenti ili građani kako bi provjerili točnost i relevantnost podataka koji se tiču upravo njih. I dok su postojale pravne sankcije za kažnjavanje značajnih zlouporaba kod rukovanja podataka, nisu postojali nikakvi zakoni koji su sadržavali pozitivne indikacije o tome kako bi trebalo pravilno organizirati i rukovati spisima s osobnim podacima.

Pravo na "**privatnost**" ili "**poštivanje privatnog života**" čuvano je kao u svetinja u međunarodnim ugovorima koji reguliraju ljudska prava nakon Drugog svjetskog rata, u novom Međunarodnom paktu o građanskim i političkim pravima (MPGPP, čl. 17) i Europskoj konvenciji o ljudskim pravima (EKLJP, čl. 8).[8] Ono štiti prvenstveno od samovoljnog miješanja države u privatni život pojedinca, kao što su presretanje komunikacija od strane državnih agencija[9] ili kriminalizacija privatnih seksualnih radnji.[10] Međutim, Europski sud za ljudska prava ovo pravo je protumačio kao obvezu države da zaštiti pojedince od objave fotografija pojedinaca koje su snimile privatne osobe, bez njihove privole, u privatnom okruženju,[11] kao i protiv presretanja njihovih

4 Hipokratova zakletva pripisuje se Hipokratu (oko 460. - 370. pr. n. e.) u starom vijeku, premda nove informacije pokazuju da je napisana nakon njegove smrti. Najstarija postojeća verzija datira negdje iz 275 g. n.e. i glasi kako slijedi: ἃ δ᾽ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα. "Što po svojem poslu budem saznao ili vidio, pa i inače, u ophođenju s ljudima, koliko se ne bude javno smjelo znati, prešutjet ću i zadržati tajnu.
Vidjeti: https://hr.wikipedia.org/wiki/Hipokratova_zakletva

5 U rimokatoličkoj crkvi, "ispovjedna tajna" ili "sakramentalni pečat" je nepovrediva. Vidjeti (eng.): https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-theconfessional.html

6 Kako kaže Regulatorno tijelo za pravne savjetnike (*the Solicitors Regulation Authority, SRA*), prilikom reguliranja djelatnosti pravnih savjetnika i odvjetničkih ureda u Engleskoj i Walesu, postoji (u engleskom pravu) "razlika između povjerljivosti i privilegije pravne profesije. U kratkim crtama, povjerljive informacije mogu se otkriti kada je to prikladno učiniti, ali privilegij nije apsolutan, te se privilegirane informacije stoga ne mogu otkrivati. Povjerljive komunikacije između odvjetnika i klijenata u svrhu dobivanja i pružanja pravnih savjeta jesu privilegirane."
https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-confidentialinformation.page
U Francuskoj, odvjetnička (*avocat*) profesionalna tajna (*secret professionnel*) pitanje je javnog poretka (*ordre public)*, apsolutna je i neograničena vremenski te obuhvaća sve vrste pravnih stvari, kao i bilo koji oblik informacija (pisane, elektroničke, zvučne, itd.). Vidjeti:
http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-confidentialite

7 Frits Hondius, A decade of international data protection (Desetljeće međunarodne zaštite podataka), u: Netherlands International Law Review (Nizozemski međunarodni pravni pregled), Vol. XXX (1983), str. 103-128 (nije dostupno online).

8 Članak 12. iz Opće Deklaracije o ljudskim pravima iz 1948. (*the Universal Declaration of Human Rights*), koja je bila instrument "majka" i za MPGPP, kao i za EKLJP (ali koja sama po sebi nije obvezujući međunarodni ugovor), već je navela u članku 12. da: "Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje..." Paralelno su pripremani MPGPP i EKLJP tijekom 1949. - 50. (ali EKLJP, koji je otvoren za potpisivanje krajem 1950. i potom stupio na snagu 1953., zapravo je stupio na snagu više od dvadeset godina prije MPGPP-a, koji je bio otvoren za potpisivanje 1966. godine i stupio na snagu tek 1976. godine).

9 Npr., ECtHR, Klass v. Germany

10 Npr., ECtHR, Dudgeon v. the UK

11 Npr., ECtHR, von Hannover v. Germany

komunikacija od strane njihovih poslodavaca bez valjane pravne osnove.[12]

Također, dok se članak 8. EKLJP-a u zadnje vrijeme sve više tumači i primjenjuje sukladno tome da štiti pojedince u pogledu njihovih osobnih podataka, te vezano za prikupljanje, korištenje i zadržavanje takvih podataka o tim pojedincima, posebno od strane državnih i nacionalnih agencija za pitanja sigurnosti,[13] tijekom 1970-ih i 80-ih godina, mjera u kojoj se može oslanjati na pravo na privatni život u odnosima između pojedinaca, te između pojedinaca i privatnih subjekata (tzv. pitanje "horizontalnog učinka ljudskih prava" ili *Drittwirkung*) i dalje je bilo vrlo nejasno[14]– te i dalje nije u cijelosti riješeno u smislu tradicionalnog zakona o ljudskim pravima. U svakom slučaju, pojedinci ne mogu izvlačiti iz EKLJP-a (ili MPGPP-a) pravo na pokretanje parnice protiv drugih pojedinaca – najviše što mogu je podnijeti tužbu protiv relevantne državne stranke jer ih je propustila zaštititi, u relevantnom nacionalnom pravu, protiv radnji takvih drugih pojedinaca.

Zaključno: Zakoni i pravila o čuvanju povjerljivosti, profesionalnim privilegiranim informacijama i njihovoj tajnosti, te jamstva ljudskih prava na privatnost i privatni život nisu ni do sada, a ni dalje na adekvatan način ne štite pojedince od zlouporabe u prikupljanju i korištenju njihovih privatnih podataka.

Posljedično, u posljednje vrijeme, postalo je priznato jedno odvojeno i zasebno pravo, pravo na "**zaštitu osobnih podataka**" ("zaštita podataka"), kao što se obrazlaže u nastavku. Ali naravno, ovo novo *sui generis* pravo mora se uvijek gledati kao usko povezano uz i komplementarno tradicionalnim pravima – kako su brižljivo očuvana u EKLJP-u i MPGPP-u posebice: zaštita podataka namjerava osigurati cjelovitu i učinkovitu primjenu tradicionalnih prava u (relativno) novom digitalnom kontekstu.

1.1.2 "Zaštita podataka"

Računala su u početku bila izrađivana u vojne svrhe tijekom **2. svjetskog rata**. Pod vodstvom velikog Alana Turinga,[15] britanski stručnjaci za dešifriranje izradili su primitivne verzije za dekriptiranje njemačke *Enigme* - i *Lorenz*-kodiranih poruka.[16]

U SAD-u, IBM je, pod vodstvom svojeg prvog glavnog direktora, Thomasa J. Watsona, proizvodio velike količine opreme za obradu podataka za vojsku i počeo eksperimentirati s analognim računalima. [17] A Nijemci su ih koristili za izračunavanje putanje *V2* raketnih projektila.[18]

Potreba za zaštitom ljudskih prava i sloboda u demokraciji u odnosu na automatiziranu obradu osobnih podataka pojavila se tek kasnije kada su, tijekom **1960-ih**, računala počela biti korištena za svrhe upravljanja u javnom i privatnom sektoru. Ali zbog visokih troškova računala i velikog prostora koji im je trebao u to doba, to je bilo učinjeno samo u razvijenim zemljama, a čak i tamo samo za velika javna tijela i društva. Ta su prva računala informatizirala lanac operacija za isplatu plaća i pružatelje usluga, registar pacijenata u bolnicama, javni popis stanovništva i statistiku – te policijske evidencije podataka.

U svjetlu takvog razvoja situacije, na **kraju 1960-ih/početkom 1970-ih**, iste su se rasprave počele voditi u Njemačkoj (posebice, u njemačkoj saveznoj pokrajini Hessen *Land*, o policijskim evidencijama podataka),

12 Npr., ECtHR, Halford v. the UK, presuda od 25. lipnja 1997.

13 Pogledati Informativni članak Vijeća Europe (Council of Europe Factsheet) – Zaštita osobnih podataka (Personal Data Protection), 2018, dostupan na: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Popis predmeta Europskog suda za ljudska prava, koji se odnose na zaštitu osobnih podataka, dostupan je na: https://www.coe.int/en/web/data-protection/echr-case-law Za općenitiju raspravu, pogledati Lee A Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, 1998, volume 6, str. 247–284, dostupno na: https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf

14 Vidjeti Hondius, o.c. (bilješka br. 7, ranije u tekstu), str. 107, s referencom na Report by the Committee of Experts on Human Rights, Vijeće Europe (DH/EXP(70)15).

15 Vidjeti: http://www.maths.manchester.ac.uk/about-us/history/alan-turing/

16 Vidjeti: Chris Smith, Cracking the Enigma code: How Turing's Bombe turned the tide of WWII, 2 November 2017, dostupno na: http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii11363990654704. Stroj Colossus koji je korišten za dekodiranje Lorenz poruka općenito se smatra "prvim svjetskim programibilnim, elektroničkim, digitalnim računalom". Vidjeti: https://hr.wikipedia.org/wiki/Colossus_(ra%C4%8Dunalo); https://en.wikipedia.org/wiki/Colossus_computer

17 Vidjeti : https://en.wikipedia.org/wiki/Thomas_J._Watson

18 Vidjeti: Helmut Hoelzer's Fully Electronic Analog Computer used in the German V2 (A4) rockets (uglavnom na njemačkom), dostupno na: http://www.cdvandt.org/Hoelzer%20V4.pdf

Norveškoj, Švedskoj i Francuskoj (posebice zbog sjećanja na zlouporabe registra popisa stanovništva i drugih javnih registara od strane *Nazi* okupatora u 2. svjetskom ratu), Ujedinjenom Kraljevstvu, SAD-u itd. – kao i u OECD-u i Vijeću Europe.[19] U početku su se te rasprave održavale između stručnjaka koji su imali etičke obveze (u SAD-u, posebice među liječnicima, koji su prvi izradili smjernice za praksu pružanja cjelovitih informacija, "*Fair Information Practices*")[20], između političara koji su bili zabrinuti zbog rizika zlouporabe ili pogrešne uporabe ili sigurnosti osobnih podataka koji se obrađuju automatski.

Oni su se potom, **sredinom i krajem 1970-ih, te ranih 80-ih**, proširili na širu populaciju – u Francuskoj, rani glavni katalizator dogodio se 1974. g. kad je došlo do otkrivanja zviždača koji su otkrili vladine planove o osnivanju nacionalne baze svih francuskih državljana i rezidenata s jedinstvenim identifikacijskim brojem za svakog od njih; a u vezi postojanja spornih policijskih evidencija podataka.[21] U Njemačkoj je postojala raširena opozicija u općenito napetoj političkoj klimi, koja je bila protiv predloženog nacionalnog popisa stanovništva 1983. godine.[22] Takve rasprave nisu se odnosile samo na rizik povrede privatnosti koja je postala moguća korištenjem novih tehnologija, već i na posljedice korištenja netočnih podataka, te na mogućnost stvaranja autoritarne vlasti centraliziranjem podataka prikupljenih za različite svrhe i/ili korištenje jedinstvenih identifikatora za međupovezivanje spisa. U Europi, ovo je dovelo do potražnje za specifičnom, zakonodavno utemeljenom "zaštitom podataka", ojačanom povećanim priznanjem ove potrebe od strane ustavnih i drugih viših sudova, kao i usvajanja međunarodnih instrumenata (kako se opisuje u odlomku 1.2 u nastavku).

Izraz "zaštita podataka" (njemački: ***Datenschutz***) izvorno je osmišljen u naslovu samog prvog zakona na tu temu, u Zakonu o zaštiti podataka iz 1970. godine (*Datenschutzgesetz*) njemačke savezne pokrajine Hessen, prema nacrtu "oca zaštite podataka", Prof. Spirosa Simitisa.[23] Kako Burkert naglašava, naziv je zapravo "netočan naziv, s obzirom da [Zakon] nije štitio podatke, već prava osoba čijim [se] podacima rukovalo".[24]

Ali izraz se "uhvatio": termin – danas poznat diljem svijeta (Francuzi ga sada također nazivaju ***protection des données***) – zapravo je skraćenica za "zaštitu pojedinaca u vezi s obradom osobnih podataka" (duža fraza koristi se i u naslovu Direktive EZ-a o zaštiti podataka iz 1995. godine i u EU-ovoj Općoj uredbi o zaštiti osobnih podataka iz 2016. godine).[25] Ali čak ni ova šira fraza u cijelosti ne razjašnjava značenje koncepta u europskim očima i mislima.

Zaštita podataka obuhvaća dvojake aspekte – aspekte osobne slobode, i društvene aspekte.

Stoga se u Francuskoj (gdje zakon sadrži pojmove "informatika, dokumenti i sloboda /informatique, fichiers et libertes) zaštita podataka smatra dijelom dualnih individualnih i društvenih te ustavnih zahtjeva:

> **obrada informacija mora biti u službi svakog građanina. ...Ona ne smije ugrožavati ljudski identitet, ljudska prava, privatni život ili individualne, odnosno javne slobode.**[26] (čl. 1 iz *Law on Informatics, Files and Freedoms* iz 1978. g.)

19 Vijeće Europe usvojilo je u svojim prvim rezolucijama o tim pitanjima tijekom 1973. i 1974.: Rezolucije Odbora ministara (73) 22 i (74) 29 (za povezniče, pogledati bilješke (fusnote) 39 i 40, u nastavku). Pogledati Obrazloženje (Explanatory Memorandum) uz Konvenciju o zaštiti podataka Vijeća Europe iz 1981., st. 6, dostupno na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca4 34 Načela iznesena u tim rezolucijama uključena su u Prilogu 1 uz priručnik. Vidjeti: Robert Gellman, Fair Information Practices: A basic history, dostupno na: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf Dugi niz godina, od 1970-ih do 1990-ih, Gellman je radio na američkim zakonodavnim pitanjima koja se tiču privatnosti u Zastupničkom domu (*the House of Representatives*).

20 Vidjeti: Robert Gellman, Fair Information Practices: A basic history, dostupno na: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf Dugi niz godina, od 1970-ih do 1990-ih, Gellman je radio na američkim zakonodavnim pitanjima koja se tiču privatnosti u Zastupničkom domu (the House of Representatives).

21 Vidjeti članak u novinama Le Monde od 21. ožujka 1974., "*SAFARI ou la chasse aux Français*" ("SAFARI, ili o lovu na sve francusko"), dostupno na: http://rewriting.net/2008/02/11/safari-ou-la-chasse-auxfrancais/ Naziv baze podataka, SAFARI, bio je akronim riječi "*système automatisé pour les fichiers administratifs et le répertoire des individus*" (Automatizirani sustav za administrativne zbirke podataka i prikupljanje zbirki podataka o pojedincima), ali je također odabran jer je ministar, nadležan za taj projekt, volio odlaziti na safari u Afriku. Otkriće su prikrile sve druge novine sljedećih dana, a vlada je zaustavila projekt nekoliko dana kasnije, imenujući *ad hoc* odbor da bi proučio čitav problem i predložio zakonita rješenja.

22 Vidjeti: Marcel Berlinghoff, *Zensus und Boykott. Die Volkszählung vor 30 Jahren*, in: Zeitgeschichteonline, lipanj 2013., dostupno na: https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

23 *Hessisches Datenschutzgesetz (HDSG) 1970*, na snazi od 13. listopada 1970., *Gesetz- und Verordnungsblatt für das Land Hessen, Teil I*, 1970, Nr. 41 (12. listopad 1970.), str. 625ff, izvorni tekst (na njemačkom) dostupno na: http://starweb.hessen.de/cache/GVBl/1970/00041.pdf

24 Herbert Burkert, Privacy-Data Protection: A German/European Perspective (nedatirano, otprilike oko 2000. g.), str. 46, dostupno na: http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

25 GDPR koristi izraz "*natural persons*" (fizičke osobe) umjesto "*individuals*" (pojedinci).

26 "*L'informatique doit être au service de chaque citoyen ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*" Ispuštena rečenica navodi da "[Zaštita podataka] treba se razviti unutar okvira međunarodne suradnje."

Taj francuski zakon dobio je ustavni status, a odluke najviših sudova u zemlji temelje se na privatnosti ili slobodi, ovisno o pitanjima o kojima je riječ.

U Njemačkoj, zaštita podataka prvenstveno se smatra izvedenom iz temeljnog (proto-) prava na "[poštivanje] ljudske osobnosti" (*das allgemeine Persönlichkeitsrecht*), jamčenog člankom 2(1) Ustava, tumačenim zajedno s čl. 1(1). Iz ovoga, Ustavni je sud, u svojoj slavnoj presudi *Census* iz 1983. godine, izveo posebnije pravo na "**informacijsko samoodređenje**" (*informationelle Selbstbestimmung*).[27] Međutim, *Bundesverfassungsgericht* je i dalje jasno i snažno povezao ovo pravo pojedinca sa širim, temeljnim društvenim normama:[28]

Društveni i pravni poredak u kojem građani više ne mogu znati tko zna što i kada o njemu i u kojoj situaciji, nekompatibilan je s pravom na informacijsko samoodređenje. Osoba koja se pita je li neobično ponašanje zabilježeno kao takvo svaki puta i potom zauvijek sačuvano u evidenciji, korišteno ili razglašavano, pokušat će ne stjecati pažnju na ovaj način. Osoba koja pretpostavlja da je, primjerice, sudjelovanje na sastanku ili u građanskoj inicijativi službeno zabilježeno, čime može doći do rizika za tu osobu, može dobrano odlučiti ne ostvarivati dotična temeljna prava ([koja su jamčena u] člancima 8 i 9 Ustava). To bi ne samo ograničilo mogućnosti za osobni razvoj pojedinca, već također i opće dobro, jer je samoodređenje ključni preduvjet za slobodno i demokratsko društvo koje se zasniva na sposobnostima i solidarnosti njegovih građana.

Druge europske države, dok ubrzano prihvaćaju potrebu za zaštitom podataka, te ga doista često uvrštavaju u svoje ustave kao *sui generis* pravo,[29] nisu sve usvojile njemački koncept informacijskog samoodređenja – često upravo zato jer smatraju da suviše stavlja naglasak na aspekt individualne slobode, a nedovoljno na one šire društvene.[30] I nadalje, u osnovi, u Europi se svi slažu da, kako je Hondius to iznio već 1983. godine:[31]

> Zaštita podataka ima za cilj čuvati pravednu i razumnu ravnotežu između interesa pojedinaca i onih zajednice [u odnosu na obradu osobnih podataka].

Europske države su zauzele stav da, kako bi se postigla ova ravnoteža, treba primijeniti sljedeća **regulatorna načela**:

- prikupljanje i daljnje korištenje te otkrivanje osobnih podataka trebalo bi biti regulirano **zakonom** (tj., **obvezujućim pravnim pravilima**, a ne dobrovoljnim pravilima ponašanja (kodeksima) ili neobvezujućim smjernicama);[32]
- ti zakoni bi trebali biti **"omnibus" zakoni** koji se načelo primjenjuju na sve javne i privatne subjekte koji obrađuju osobne podatke (s iznimkama i modifikacijom tih pravila i načela predviđenima u posebnim pravilima, ovisno o potrebi i kada je potrebno, ali uvijek poštujući njihovu "temeljnu srž");
- dotični zakon mora sadržavati određena **temeljna materijalna pravila** (koja odražavaju **"srž" načela zaštite podataka** o kojima se govori pod sljedećim naslovom) i jamčiti ispitanicima **ključna individualna prava**; te
- primjenu tih zakona trebaju nadzirati **posebna nadzorna tijela** (obično nazvana **nadzornim tijelima za zaštitu podataka** ili **TZP-ovi**).

---

27 BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 ff. O pitanju "informacijskog samoodređenja", vidjeti čl. 151ff.
28 *Idem*, § 154 (naš prijevod).
29 Cf. austrijski zakon o zaštiti podataka iz 1978. godine, koji sadrži "ustavnu" odredbu u svojem prvom članku, proglašavajući zaštitu podataka ustavom zaštićenim pravom. Zaštita podataka je također izrijekom predviđena u ustavima Španjolske (čl. 18-4), Portugala (čl. 35), Grčke (čl. 9A), Mađarske (čl. 59), Litve (čl. 22), Slovenije (čl. 38), Slovačke (čl. 19) i Nizozemske (čl. 10).
30 Vidjeti, npr., blog *Informationelle Selbstbestimmung - (noch) kein neues Grundrecht*, 26. listopada 2017. godine, o odbijanju nižeg doma švicarskog saveznog parlamenta (*Nationalrat*) da uključi načelo informacijskog samoodređenja u švicarski savezni ustav: https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelleselbstbestimmung
U Nizozemskoj, također, načelo nije usvojeno ni u zakonu ni od strane sudova – premda je praksa njemačkog ustavnog suda pored toga utjecala na najviši sud, *Hoge Raad*. Vidjeti: T. F. M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens (2001), odlomak 4.3 (str. 18).
31 Hondius, o.c. (bilješka (fusnota) 7, prethodno u tekstu), str. 108.
32 Usp. tumačenje koncepta "zakona" u Europskoj konvenciji o ljudskim pravima (posebice članci 8 – 11), od strane Europskog suda za ljudska prava.

1.2 PRVI ZAKONI O ZAŠTITI PODATAKA, NAČELA I MEĐUNARODNI INSTRUMENTI33

1.2.1 Prvi zakoni o zaštiti podataka

"Zapadna Europa je kolijevka zaštite podataka"[34]

Kako je spomenuto, prvi zakon o zaštiti podataka na svijetu bio je ***Datenschutzgesetz* njemačke savezne pokrajine Hessen, koji je usvojen u rujnu 1970. godine**.[35] Taj je zakon također uveo prvo neovisno tijelo za zaštitu podataka (premda, zbog pitanja nadležnosti države, samo za javni sektor i više s ograničenim ovlastima medijacije nego provedbe). Nakon usvajanja Zakona o zaštiti podataka iz Hessena, u Europi je uslijedilo usvajanje nacionalnih (diljem države) zakona o zaštiti podataka u Švedskoj (1973. **g.)**, prvi **njemački Savezni zakon o zaštiti podataka (krajem 1977. godine)** (koji je obuhvaćao obradu osobnih podataka od strane saveznih agencija i od strane privatnog sektora), **francuski *Zakon o obradi informacija i slobodama* od 6. siječnja 1978. g.**, zakoni u **Austriji**, **Danskoj**[36] i **Norveškoj (svi također 1978. g.)** i **Luxembourgu (1979. g.)**. Premda su neki od ovih, kao primjerice njemački Savezni zakon, sadržavali zasebni komplet pravila za (savezni) javni i privatni sektor, oni su i dalje "omnibus" zakoni, jer se pravila za oba sektora zasnivaju na istim osnovnim načelima i pravima, često izvedenima iz ustava.

1.2.2 Osnovna načela

Europski zakoni iz 1970-ih kombiniraju sve više općeprihvaćene (široko frazirane) **komplete "ključnih" načela i prava**. Oni su bili slični osnovnim načelima prakse pružanja cjelovitih informacija, "*Fair Information Practices*", koja su sastavljena negdje u to doba u SAD-u (iako je ta praksa bila manje detaljna i nije bila navedena u obvezujućim zakonima). [37]

Ova ključna načela ranih zakona iz Europe bila su pak reflektirana u **najranijim (neobvezujućim) europskim instrumentima** o tom pitanju, koja je izdalo Vijeće Europe (i koje je potom postalo osnova za kasniju, obvezujuću Konvenciju Vijeća Europe o zaštiti podataka):

- Rezolucija Vijeća Europe iz 1973. godine (73)22 o Zaštiti privatnosti pojedinaca vis-à-vis elektroničkih banki podataka u privatnom sektoru, koju je usvojio Odbor ministara 26. rujna 1973. g.;[38]
- Rezolucija Vijeća Europe iz 1974. godine (74)29 o Zaštiti privatnosti pojedinaca vis-à-vis elektroničkih banki podataka u privatnom sektoru, koju je usvojio Odbor ministara 20. rujna 1974. g.[39]

---

33 Radi iznošenja povijesnih detalja, s posebnim ukazivanjem na izradu paralelnih OECD-ovih Smjernica 1980. godine i Konvencije o zaštiti podataka Vijeća Europe 1981. godine, te na već tada prisutne razlike u stajalištima između Europe i SAD-a, vidjeti: Frits Hondius, o.c. (bilješka (fusnota) 7, ranije u tekstu), str. 103-128, i Obrazloženje uz Konvenciju Vijeća Europe (Explanatory Memorandum to the Council of Europe Convention), o.c. (bilješka (fusnota) 19, ranije u tekstu), st. 14. Iznimno koristan opći pregled povijesnih događanja u pitanjima privatnosti iznesen je u Poglavlju 4 ažuriranog OECD-ovog Privacy Framework, pod naslovom The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (Evoluirajuće okruženje privatnosti: 30 godina nakon Smjernica o privatnosti OECD-a), detaljnije opisan u nastavku (vidjeti bilješku (fusnotu) 40). Fascinantan osobni opis pozadine izrade OECD-ovih Smjernica i politika (Europa nasuprot SAD-u) i uključene osobe (uključujući Fritsa Hondiusa, Louisa Joineta, Stefana Rodotu i Spirosa Simitisa), iznosi Michael Kirby, (Privatnost danas: Nešto novo, nešto staro, nešto posuđeno, nešto plavo, eng. Privacy Today: Something Old, Something New, Something Borrowed, Something Blue, Journal of Law, Information and Science, 2017
25(1), dostupno na: http://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

34 Hondius, o.c. (bilješka (fusnota) 7, prethodno u tekstu), str. 104, s pozivom na prethodno zakone spomenute u tekstu.

35 Vidi bilješku (fusnotu) 23, prethodno u tekstu. Za daljnje reference o povijesti zaštite podataka u Njemačkoj, Vidjeti: Herbert Burkert, o.c. (bilješka (fusnota) 24, prethodno u tekstu).

36 U Danskoj, u početku su postojala dva zakona, jedan za privatni sektor, a drugi za javni sektor, usvojeni na isti dan (Zakoni br. 293 i 294, oba od 8. lipnja 1978. g.), ali i dalje oba temeljena na istim širokim načelima. Radi dobivanja uvida u pozadinu istoga, vidjeti *Introduction* (*Uvod*) u: Peter Blume, Person-registrering, Copenhagen, 1991. Oba su ostala na snazi, s različitim izmjenama, sve do 2000. godine, kada je doneseno novo zakonodavstvo u cilju provedbe Direktive o zaštiti podataka iz 1995. godine.

37 Odvojeni državni zakoni o zaštiti podataka (*Landesdatenschutzgesetze)* obuhvaćaju državne javne sektore, ali se temelje na jednakim načelima, ukorijenjenima u Ustavu.

38 Dostupno na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805028 30

39 Dostupno na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c 51

"Ključna" načela bila su potom priznata u **globalnim međunarodnim, ali i dalje neobvezujućim, instrumentima**, tj.:

- Smjernice mjerodavne za zaštitu privatnosti i prekogranični protok osobnih podataka OECD-a iz 1980. g.;[40] i
- Smjernice UN-a za reguliranje računalnih zbirka osobnih podataka iz 1989. g., koje je usvojila Opća skupština Ujedinjenih naroda (UNGA).[41]

Temeljna načela iz gornja četiri neobvezujuća međunarodna instrumenta donesena 1970-ih i 80-ih, te načela iz američke prakse pružanja cjelovitih informacija, "*Fair Information Practices*" iz 1973. g., upućujemo na poveznice u bilješkama.

Ovdje je dovoljno napomenuti da svi imaju za cilj rješavanje inherentnog problema s računalima: da po svojoj prirodi olakšavaju mnoge nove uporabe podataka, uključujući osobne podatke, bez ograničenja sigurnosti i upotrebe, što je inherentan aspekt njihove specifičnosti. Drugim riječima, osnovna načela nastoje spriječiti zlouporabe osobnih podataka koje nove tehnologije čine previše jednostavnim ako ih se ne provjerava. U tom smislu, oni ostaju smisleni.

Za potrebe ovog teksta, dostatno je samo iznijeti ona koncizno sročena u OECD-ovim Smjernicama.

OECD-ova načela iz 1980. g.

- **Načelo ograničenja prikupljanja**

Trebaju postojati ograničenja u pogledu prikupljanja osobnih podataka i bilo koji takvi podaci trebaju se pribaviti zakonitim i pravednim sredstvima, te, kada je to primjenjivo, uz znanje ili privolu ispitanika.

- **Načelo kvalitete podataka**

Osobni podaci trebali bi biti relevantni svrhama u koje se koriste, i, u mjeri potrebnoj za postizanje tih svrha, trebaju biti točni, potpuni i vođeni ažurno.

- **Načelo navođenja svrhe**

Svrhe u koje se osobni podaci prikupljaju trebaju biti navedene najkasnije u doba prikupljanja podataka, a naknadno korištenje treba biti ograničeno na postizanje tih svrha ili takvih drugih svrha koje nisu nespojive s tim svrhama, te kako su navedene prilikom svake promjene svrhe.

- **Načelo ograničenja korištenja**

Osobni podaci se ne bi smjeli priopćavati, učiniti dostupnima niti na drugi način koristiti u svrhe osim onih koje su sukladno navedene [ranijem načelu] s iznimkom:

a) uz privolu ispitanika; ili
b) na zahtjev zakonite vlasti.

- **Načelo odgovarajuće razine zaštite**

Osobni podaci trebaju biti zaštićeni razumnim sigurnosnim zaštitama od takvih rizika ili gubitaka ili neovlaštenog pristupa, uništenja, korištenja, izmjene ili otkrivanja podataka.

40 OECD, Preporuka Vijeća koja se tiče Smjernica koje su mjerodavne za zaštitu privatnosti i prekogranični protok osobnih podataka, 23. rujan 1980. g., dostupno na: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonal data.htm Za objašnjenje pozadine, pogledati Kirby, o.c. (bilješka (fusnota) 33, ranije u tekstu). S naglaskom na to da su OECD-ove Smjernice revidirane 2013. godine u kontekstu stvaranja šireg OECD-ovog Okvira privatnosti koji također uključuje nova pravila o suradnji kod provedbe privatnosti, koja se temelje na preporukama o tom pitanju iz 2007. g., Pogledati: https://www.oecd.org/sti/ieconomy/privacy.htm Ali to nema učinka na osnovna načela iz 1980-ih.

41 Ujedinjeni narodi, Smjernice za reguliranje kompjuteriziranih zbirki osobnih podataka, UNGA Res. 44/132, 44 UN GAOR Supp. (br. 49) na 211, UN Doc. A/44/49 (1989), dostupno na: https://www1.umn.edu/humanrts/instree/q2grcpd.htm, s naglaskom na to da je ovo prvi instrument koji priznaje potrebu za neovisnim tijelima za zaštitu podataka.

- **Načelo otvorenosti**

Treba postojati opća politika (pravila) otvorenosti o razvoju, praksama i politikama u pogledu osobnih podataka. Sredstva trebaju biti lako dostupna za utvrđivanje postojanja i prirode osobnih podataka, kao i glavnih svrha njihovog korištenja, kao i identiteta i uobičajenog boravišta voditelja obrade podataka.

- **Načelo individualnog sudjelovanja**

Pojedinac treba imati pravo:

a) dobiti od voditelja obrade podataka, ili na drugi način, potvrdu o tome ima li voditelj obrade podataka ili nema podatke koji se odnose na tog pojedinca;

a) da mu priopći podatke koji se odnose na njega unutar razumnog roka; uz naplatu, ako takva postoji, koja nije prekomjerna; na razuman način; i u obliku koji mu je lako razumljiv;

a) da mu se navedu razlozi ako nije udovoljeno zahtjevu postavljenom sukladno točkama (a) i (b), te biti u mogućnosti osporiti takvo neispunjenje zahtjeva; i

b) osporiti podatke koji se odnose na njega i, ako je osporavanje uspješno, imati mogućnost da se podaci izbrišu, isprave, upotpune ili izmijene.

- **Načelo pouzdanosti**

Voditelj obrade podataka treba odgovarati za usklađenost s mjerama koje daju učinak načelima navedenima ranije.

Važno je naglasiti da načela (u svim instrumentima) trebaju uvijek biti shvaćana i primijenjena zajedno: samo tada ona mogu pružiti ozbiljnu zaštitu od zlouporaba ili pogrešne uporabe osobnih podataka, kao što su greške u digitaliziranim ili pohranjenim podacima, prikupljanje više podataka negoli je potrebno ili zadržavanje tih podataka duže no što je potrebno, korištenje podataka za različite svrhe, krađa ili otkrivanje podataka trećim osobama u nezakonite svrhe, gubitci podataka, *hakiranje* itd.

1.2.3 Konvencija Vijeća Europe o zaštiti podataka iz 1981. godine i njezin Dodatni protokol

Prvi obvezujući međunarodni instrument na području zaštite podataka bio je Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka Vijeća Europe iz 1981. g., bolje poznata kao Konvencija o zaštiti podatka (DPC) ili "Konvencija br. 108" prema njenom broju u Seriji europskih međunarodnih ugovora.[42] Kao Konvencija Vijeća Europe (a ne "europska Konvencija"), Konvencija o zaštiti podataka je otvorena za ratifikaciju i državama koje nisu članice Vijeća Europe, na poziv (čl. 23). Do današnjeg dana (kolovoz 2018. g.), Konvenciju je ratificiralo svih 47 država članica Vijeća Europe, te šest neeuropskih država (Urugvaj [2013.], Mauricijus [2016.], Senegal [2016.], Tunis [2017.], Zelenortski otoci (Cabo Verde) i Meksiko [2018.]).[43] Dvije dodatne neeuropske države pozvane su pridružiti se Konvenciji: Argentina i Burkina Faso.[44] Konvencija je 2001. g. proširena Dodatnim protokolom.[45]

Konvencija iz 1981. i taj Dodatni protokol ukratko su opisani u nastavku u prošlom vremenu jer nedavno, tijekom 2018. g., oni su temeljitije izmijenjeni ("modernizirani") u daljnjem protokolu, kako se opisuje u odlomku 1.3, u nastavku. Međutim, treba naglasiti da će se revidirana ("modernizirana") Konvencija" primijeniti

42 Puni naziv: Vijeće Europe, Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, otvorena za potpisivanje u Strasbourgu na dan 28. siječnja 1981. g., CETS br. 108, dostupno: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

43 Vidjeti: https://www.coe.int/en/web/conventions/search-on-treaties//conventions/treaty/108/signatures?p_auth=qsJbzlEi

44 *Idem.*

45 Puni naziv: Vijeće Europe, Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u svezi nadzornih tijela i međunarodne razmjene podataka, otvoren za potpisivanje u Strasbourgu na dan 8. studeni 2001. g., CETS br. 181, dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626

Dodatni protokol je ratificiralo 36 država članica od ukupno 47 država članica Vijeća Europe, kao i šest nečlanica (Zelenortski otoci, Mauricijus, Meksiko, Senegal, Tunis i Urugvaj). Burkina Faso je pozvana pristupiti. Vidjeti:
https://www.coe.int/en/web/conventions/search-on-treaties//conventions/treaty/181/signatures?p_auth=yDDCP83k

samo na one države stranke koje joj pristupe: za ostale, nastavlja se primjenjivati tekst iz 1981. g. (zajedno s Dodatnim protokolom kad je to primjenjivo).

Kao obvezujući međunarodni instrument, Konvencija iz 1981. g. (za razliku od ranijih neobvezujućih instrumenata) morala je, i prigodno jest, uključiti preciznije pravne **definicije** glavnih koncepata u pravu zaštite podataka: "**osobni podatak**", "**voditelj zbirke podataka**" i "**obrada**" (iako su u kasnijim instrumentima ovi koncepti trebali biti, i doista jesu, prošireni i dopunjeni) (čl. 2).

Glavna načela zaštite podataka obrazložena ranije - **načelo ograničenja prikupljanja**, **načelo kvalitete podataka**, **načelo navođenja svrhe** i **načelo ograničenja korištenja** – izneseni su u članku 5. Konvencije iz 1981. g. (bez korištenja tih izraza: Konvencija navodi ta načela zajedno pod naslovom "*Svojstvo podataka*"). **Načelo sigurnosti podataka** (u Konvenciji navedeno kao "*Sigurnost podataka*", tj. *Security Safeguards Principle*) izneseno je u članku 7; a **načela otvorenosti i osobnog sudjelovanja** izneseni su u članku 8. (pod naslovom "*Dodatna jamstva za ispitanika*").[46]

Konvencija je ovim navedenima, dodala poseban članak o obradi podataka "**posebne kategorije podataka**", tj., "*podaci koji otkrivaju rasno podrijetlo, politička mišljenja, vjerska ili druga uvjerenja, kao i osobni podaci koji se tiču zdravlja ili spolnog života*" i "*osobni podaci koji se odnose na kaznene presude*" (čl. 6). Konvencija navodi da se takvi podaci – uobičajeno zvani "**osjetljivi podaci**" – "*ne mogu automatizirano obrađivati ako unutarnje pravo ne predviđa primjerenu zaštitu*".

NB: Potreba za posebnim pravilima za određene vrste podataka bila je žustro diskutirana u to doba. Neki su, uključujući Simitisa, smatrali da bilo koji podaci mogu biti osjetljivi, ovisno o kontekstu, dok neki od navedenih podataka mogu biti bezopasni u drugim kontekstima. Drugi su smatrali da samo uporaba osjetljivih podataka treba biti regulirana, jer je uporaba osjetljivih podataka inherentno rizična i može dovesti do diskriminacije. Na kraju je prevagnuo prijedlog kojeg je iznio Louis Joinet, francuski predstavnik i predsjedavajući odbora Vijeća Europe zadužen za izradu instrumenta,[47] i uporaba svih osobnih podataka je regulirana, s povišenim stupnjem zaštite za osjetljive podatke.

U isto vrijeme, Konvencija je omogućila državama strankama Konvencije da usvoje **iznimke i ograničenja** za većinu zahtjeva iz Konvencije (ali ne za zahtjeve koji se tiču sigurnosti

podataka), radi "***zaštite državne sigurnosti, javne sigurnosti, monetarnih interesa države ili suzbijanja kaznenih djela***" ili "***zaštite subjekta podataka ili prava i slobode drugih***", pod uvjetom da je odstupanje "predviđeno ***pravom*** Države stranke" i da "predstavlja ***nužnu*** mjeru u demokratskom društvu" za zaštitu tih interesa (čl. 9(2)).[48]

Osim davanja pravnog učinka ključnim načelima zaštite podataka (uz dodatak posebnih pravila o osjetljivim podacima) i pravima subjekata podataka, Konvencija iz 1981. g. je također potvrdila dva od gore navedenih europskih **regulatornih zahtjeva**:

- Tražilo se od država stranaka da primijene njene odredbe u **obvezujućim zakonskim pravilima**. To se moglo u formi zakona, propisa ili administrativnih odredbi, a moglo ih se dopuniti neobvezujućim smjernicama ili pravilima ponašanja (kodeksima) – ali glavna pravila sama po sebi morala su biti u obliku "obvezujućih mjera".[49]

46 Obzirom da primjena ključnih načela predstavlja primarnu zaštitu pojedinaca, prava ispitanika su komplementarna istima. Prava pojedincu omogućavaju veću kontrolu nad upotrebom njegovih osobnih podataka.

47 Louis Joinet bio je, sve do umirovljenja, viši francuski sudac koji je bio član ad hoc komisije za izradu francuskog zakona o zaštiti podataka iz 1978. godine, prije nego li je postao prvi direktor francuskog DPA-a (CNIL). Bio je zadužen za izradu UN-ovih Smjernica (bilješka (fusnota) 42, ranije u tekstu) i postao je vrlo ugledan francuski zastupnik u Odboru za ljudska prava UN-a. Pogledati: https://fr.wikipedia.org/wiki/Louis_Joinet http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

48 U pravu EKLJP-a zahtjev proporcionalnosti pročitan je u izričito propisanom zahtjevu nužnosti (u demokratskom društvu), dok se u pravu EU - osobito u Povelji o temeljnim pravima EU - dva pojma rješavaju kao zasebna (iako još uvijek srodnih načela: usp. čl. 52 PTP.

49 Explanatory Memorandum to the Council of Europe Convention (Obrazloženje uz Konvenciju Vijeća Europe), o.c. (bilješka (fusnota) 19, prethodno u tekstu), st. 39.

- Tražilo se od država stranaka da primijene svoje zakone široko, **na (sve) "automatizirane zbirke podataka i automatiziranu obradu osobnih podataka u javnom i u privatnom sektoru"** (čl. 3(1)). Drugim riječima, barem načelno, zahtijevalo se usvajanje **"omnibus" zakona**.[50]

Međutim, Konvencija iz 1981. g. još nije zahtijevala od država stranaka da ustanove neovisno **tijelo za zaštitu podataka**. Također se još nije pozabavila pitanjem koje je ubrzo postalo istaknuto u svjetlu sve većeg prekograničnog protoka podataka: **potreba za ograničenjem takvih prekograničnih protoka podataka** kako bi se spriječilo zaobilaženje materijalnih pravila ključnih prava subjekata podataka (ispitanika), nametanjem pravila kako bi se osiguralo da će se zaštita nastaviti primjenjivati i nakon što su podaci napustili teritorij neke države koja ima odgovarajuće zakone o zaštiti podataka.

Umjesto toga, Konvencija iz 1981. g. regulirala je jedino da države stranke:

> ne mogu, isključivo u svrhu zaštite privatnosti, zabraniti ili podvrgnuti posebnom odobrenju prekogranični protok osobnih podataka usmjeren za područje druge stranke (čl. 12(2)).

osim ako je država stranka u tom slučaju usvojila stroža pravila za dotičnu kategoriju podataka, ili je prijenos u drugu državu stranku izvršen s namjerom da se takvim prijenosom zaobiđe zakonodavstvo stranke navedene na početku ovog stavka (čl. 12(3)).

Drugim riječima, Konvencija iz 1981. g. nije se bavila pitanjem prijenosa u države koje nisu stranke Konvencije.

Na kraju, može se zamijetiti da se Konvencija primjenjivala samo na "automatizirane zbirke podataka i automatiziranu obradu osobnih podataka" (čl. 3(1), usp. također čl. 1). Drugim riječima, **zbirke osobnih podataka koje nisu predmet automatizirane obrade**, uključujući "strukturirane ručno vođene evidencije", još nisu bile podložne primjeni njenih odredbi (iako su Države stranke mogle odabrati proširiti primjenu Konvencije na takve zbirke: čl. 3(2)(c)).

Dvije su manjkavosti ispravljene u Dodatnom protokolu uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u svezi nadzornih tijela i međunarodne razmjene podataka, usvojenom 2001. godine (već spomenuto),[51] koji, kako se vidi iz naslova, zahtijeva ustanovljavanje **neovisnih TZP-ova s ovlastima za poduzimanje istrage i posredovanja, kao i pokretanja pravnih postupaka** (čl. 1), te nametanje **načelne zabrane protoka osobnih podataka u državu koja ne osigurava "odgovarajuću razinu zaštite"** (čl. 2). Dodatni protokol usvojen je uvelike kako bi uveo uređenje u Konvenciju bliže uređenju sukladno tada važećoj Direktivi EZ-a o zaštiti podataka iz 1995. g., o čemu se govori u odlomku 1.3, dalje u tekstu.

Prilično nedavno, u svibnju 2018. g., Konvencija iz 1981. g. je dalje "**modernizirana**", kako bi se više uskladila s nedavnim EU zakonodavstvom o zaštiti podataka i općenitim (globalnim) razvojem zaštite podataka, kako se dalje obrazlaže pod točkom 1.4.3, dalje u tekstu.

Unutar Vijeća Europe, brojna se tijela bave pitanjima zaštite podataka, uključujući Parlamentarnu skupštinu Vijeća Europe (PACE), Savjetodavni odbor, poznat kao "T-PD", ustanovljen Konvencijom br. 108 – koji ima glavnu odgovornost za svakodnevni nadzor razvoja koji se odnosi na zaštitu podataka, te za razradu nacrta sektorskih i drugih smjernica i preporuka u ovom području – kao i Odbor ministara Vijeća Europe (COM ili CM), koji potom usvaja posebice te prijedloge. Unutar tih tijela, izdana su mnoga mišljenja, preporuke i studije u tom području – uvijek s pozivom na Konvenciju.[52]

---

50 Ovo podliježe primjeni odredbe da bilo koja država stranka može izjaviti "da neće primjenjivati ovu Konvenciju na određene kategorije automatiziranih zbirki osobnih podataka" (čl. 3(2)(a)).

51 Vidjeti bilješku (fusnotu) 46, prethodno u tekstu.

52 Vidjeti: http://website-pace.net/en_GB/web/apce/documents (PACE dokumenti). Primijetite da ti dokumenti obuhvaćaju mnogo više pitanja negoli samu zaštitu podataka – ali može ih se pretraživati upisivanjem izraza "data protection".
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (T-PD dokumenti);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (COM dokumenti koji se odnose na zaštitu podataka).

Pored toga, postoji i međusobni utjecaj između Konvencije za zaštitu podataka i Europske konvencije o ljudskim pravima, pri čemu Europski sud za ljudska prava sve više uzima u obzir Konvenciju za zaštitu podataka, kao i ranije navedene vrste dokumenata u svojem vlastitom tumačenju članka 8. Konvencije o ljudskim pravima (koji jamči pravo na privatni život); dok se za to vrijeme PACE, Savjetodavni odbor i Odbor ministara zauzvrat oslanjaju na sudsku praksu Suda u svojem radu na tom području.[53]

53 Vidjeti Vijeće Europe Informativni članak (Factsheet) – personal data protection (bilješka (fusnota) 13, prethodno u tekstu) i *Dodatak* (*Annex) 1 – Jurisprudence* uz radni dokument EU-ove "Radne skupine iz članka 29", Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (RS237), usvojen 13. travnja 2016., koji navodi popis od 15 važnih ECtHR presuda bitnih za zaštitu podataka (i pet presuda SEU-a), dostupno na:

1.3 EUROPSKO PRAVO ZAŠTITE PODATAKA TIJEKOM 1990-IH I RANIH 2000-IH

1.3.1 Zaštita podataka u Europskoj zajednici

POZADINA

Neko je vrijeme Europska zajednica (to je tadašnji naziv za EU)[54] osjećala da je Konvencija Vijeća Europe o zaštiti podataka iz 1981. g. pružila dostatnu zaštitu u tom području. Međutim, do kraja tog desetljeća, postalo je jasno da Konvencija nije dovela do velike ni široko harmonizirane zaštite osobnih podataka u Zajednici: do rujna 1990. g. ratificiralo ju je samo sedam država članica EZ-a (od kojih jedna zapravo još nije usvojila relevantno zakonodavstvo), a zakoni u tim državama članicama značajno su se razlikovali u važnim aspektima.[55] U to doba, Italija je imala samo zakon o zaštiti podataka u odnosu na radnike, Španjolska nije imala "omnibus" zakon iako je predvidjela zaštitu podataka kao temeljno pravo u svojem Ustavu itd.

To je bilo u skladu s općim trendom u Europskoj zajednici u to doba, harmonizirati sve oblike pravila i zakona kako bi se olakšalo otvaranje unutarnjeg tržišta, s njegovim predloženim slobodnim kretanjem roba, usluga, kapitala i osoba. Konkretnije, tijekom međunarodne konferencije o zaštiti podataka iz 1989. godine u Berlinu, Europska komisija je obavijestila okupljene predstavnike o usklađivanju pravila za sektor telekomunikacija. To je pokazalo da je postalo ključno imati i dobro primjenjive, snažne zakone o zaštiti podataka u svim državama članicama.[56]

Podrobnije, tijekom konferencije 1989. g., Europska je komisija obavijestila okupljene zastupnike tijela EZ-a za zaštitu osobnih podataka da se sprema harmonizacija pravila za sektor telekomunikacija. To je pokazalo da je od ključne važnosti imati dobro primijenjene, snažne zakone o zaštiti podataka u svim državama članicama.

Kao izravan rezultat ove inicijative, sljedeće godine, u rujnu 1990. g., Europska komisija je stoga iznijela ambiciozan, niz prijedloga, usmjeren na zaštitu osobnih podataka kroz prvi stup[57].

---

54 U doba uvođenja paketa prijedloga Komisije, o kojima se raspravlja u ovom odlomku (rujan 1990.g.), Komisija je i dalje formalno bila "Komisija Europskih zajenica" (množina). Izraz "Europska zajednica" (jednina) počeo se primjenjivati tek 1992.g., prema Ugovoru iz Maastrichta, sve do stupanja na snagu Ugovora iz Lisabona 2009. godine. Međutim, pojednostavljenja radi, mi ćemo općenito govoriti o Europskoj zajednici u ovom odlomku, odnosno o Europskoj uniji u sljedećem, odlomku 1.4, te u Drugom i Trećem dijelu.

55 Komisija Europskih zajednica, Priopćenje o zaštiti pojedinaca vezano za obradu osobnih podataka u Zajednici i sigurnosti informacija, COM(90)314 konačna verzija – SYN287 i 288, Brussels, 13. rujna 1990. g., *Introduction (Uvod)*. Cjeloviti dokument je dostupan *online* iz odličnog arhiva Centra za intelektualno vlasništvo i informacijsko pravo kod *the Cambridge University*, na poveznici: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communi cation.pdf. Posebno vidjeti st. 6 – 8.

56 Na Berlinskoj konferenciji, Spiros Simitis, povjerenik za zaštitu podataka za njemačku zemlju Hessen (i inicijator prvog zakona o zaštiti podataka na svijetu u toj državi) javno je pozvao Jacquesa Fauveta, tadašnjeg predsjednika francuskog tijela za zaštitu podataka. CNIL (i prethodno voditeljica novina "Le Monde"), kako bi tada pisali svom dugogodišnjem prijatelju Jacquesu Delorsu, tadašnjem predsjedniku Europske komisije, da poduzme inicijativu za usklađivanje zakona o zaštiti podataka unutar EK.

57 Ugovorom o Europskoj uniji, potpisanom 7. veljače 1992. godine u Maastrichtu (Ugovor iz Maastrichta), predviđena je uspostava trostupnestrukture pod jedinstvenom upravom. Prvi stup sastojao se od Europske ekonomske zajednice (EEC), Europske zajednice za ugljen i čelik (ECSC) te Europske zajednice za atomsku energiju (EAEC) (iako je svaki od njih zadržao pravnu osobnost) te je pokrivao jedinstveno tržište kreirano 1993. godine. Drugi i treći stup obuhvaćali su zajedničku vanjsku i sigurnosnu politiku (ZVSP) te suradnju na području pravosuđa i unutarnjih poslova (PUP). Stupovi su formalno ukinuti Lisabonskim ugovorom, međutim zasebni instrumenti se još uvijek izdaju za određena područja (usporedi: rasprava o opsegu GDPR-a u drugom dijelu, odlomak 2.3). Posjetiti web stranicu istraživačkog centra CVCE. Sveučilišta u Luxembourgu, a posebno stranicu naslova "Prvi stup Europske unije": https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274. Direktiva o zaštiti podataka 1995 (kao i ostale prethodno spomenute direktive) izdana je u vrijeme postojanja prvog stupa te je (kao i prethodno spomenute) bila izdana samo u tu svrhu. Mjere zaštite podataka u ostala dva stupa naznačene su u pododlomcima 1.3.4 i 1.3.5, u nastavku, dok su pravila zaštite podataka namijenjena institucijama EU općenito, naznačena u pododlomku 1.3.6.

Paket je uključivao prijedloge za dvije direktive, tj.: [58]

- **opća direktiva EZ-a** (tj., pravni instrument ograničen na ono što je tada bilo "prvi stup" Europske zajednice) "*o zaštiti pojedinaca u vezi s obradom osobnih podataka*" – koja je nakon poduljeg zakonodavnog procesa postala glavna Direktiva o zaštiti podataka EZ-a, Direktiva 95/46/EZ, o kojoj se govori u nastavku, pod točkom 1.3.2; i
- predložena potom, **pomoćna EU direktiva** "*o zaštiti osobnih podataka u kontekstu javnih digitalnih telekomunikacijskih mreža, posebice digitalnih mreža s integriranim uslugama (ISDN) i javnim digitalnim mobilnim mrežama*" – koja je postala Direktiva o obradi osobnih podataka i zaštiti privatnosti u području telekomunikacija, Direktiva 97/66/EZ, usvojena u prosincu 1997. g., od tada zamijenjena Direktivom 2002/58/EZ, tzv. "Direktivom o e-privatnosti", o kojoj se govori u nastavku, pod točkom 1.3.3;

Prije rasprave o ovim dvjema direktivama, važno je zamijetiti prirodu i svojstva ograničenja takvih instrumenata.

PRIRODA I OGRANIČENJA EZ DIREKTIVA

Kod rasprave o glavnim EZ instrumentima o zaštiti podataka, a posebice o gore navedenim direktivama o zaštiti podataka, potrebno je tri stvari imati na umu. Prvenstveno, bilo koji EU (ili ranije: EZ) pravni instrument jest, po samoj svojoj prirodi, ograničen na teme unutar djelokruga prava EU-a (ili ranije: EZ-a). Određene teme, ponajviše aktivnosti država članica u odnosu na **nacionalnu sigurnost**, (gotovo) su u cijelosti izvan djelokruga prava EU-a (ili ranije: EZ-a)[59] te nikakvi pravni instrumenti EU-a (ili EZ-a) (uključujući ove direktive – ili sami GDPR, ni bilo koja buduća pravila o zaštiti podataka u EU, u bilo kojem obliku) stoga nisu primjenjivi na takve aktivnosti. Ovo je izrijekom potvrđeno u direktivama (i u GDPR-u): vidjeti članak 3(2) iz Direktive o zaštiti podataka iz 1995. g. i članak 1(3) iz Direktive o e-privatnosti (i čl. 2(2)(a) GDPR-a).[60]

Drugo, EZ direktive o kojima se raspravlja u nastavku, ograničene su na područje unutar tzv. **prvog stupa**[61] te po samoj prirodi EZ direktiva, nisu bile primijenjene na aktivnosti iz drugog ili trećeg stupa, za koje su izrađeni odvojeni instrumenti zaštite podataka spomenuti u pododlomcima 1.3.4 i 1.3.5 u nastavku, ali o kojima se ne raspravlja dalje u ovom prvom izdanju priručniku. Dostatno je primijetiti da *bilo koje prosljeđivanje osobnih podataka ili činjenje istih dostupnima* od strane osoba na koje se primjenjuju direktive (uključujući i osobe u privatnom sektoru i od javnih tijela koja provode aktivnosti na koje se primjenjuje pravo prvog stupa (EZ)), bilo kojoj agenciji za provedbu zakona ili nacionalnu sigurnost bilo je (a u slučaju Direktive o e-privatnosti, i dalje jest) podložno tim instrumentima (jer su takva otkrivanja podataka predstavljala "obradu" u smislu

58 Komisija Europskih zajednica, Priopćenje o zaštiti pojedinaca vezano za obradu osobnih podataka u Zajednici i sigurnosti informacija (ranija bilješka (fusnota)). Paket je sadržavao četiri daljnja prijedloga, tj.:

- nacrt **rezolucije** predstavnika Država članica koji bi proširio primjenu načela sadržanih u općoj direktivi na zbirke koje vode tijela s javnim ovlastima na koje se glavna Direktiva o zaštiti podataka kao takva ne bi primjenjivala – a koja nikada nije usvojena kao takva, ali se može sagledati kao geneza pravila o zaštiti podataka koja se odnose na provedbu zakona i pravosudne predmete, u najnovije doba kumulirano u Direktivi o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka, tj. *the Law Enforcement Data Protection Directive* (Direktiva (EU) 2016/680 (o njoj se ne raspravlja u ovom priručniku: vidjeti Bilješku u okviru "*O ovom priručniku*" na str. 1, ranije u tekstu);
- nacrt **deklaracije** Komisije o primjeni standarda zaštite podataka iznesenih u glavnoj Direktivi o zaštiti podataka za zbirke koje vode same institucije Zajednice – što je u konačnici dovelo do Uredbe (EZ) 45/2001 (*idem*);

- **preporuka za odluku Vijeća** o pristupanju Europske zajednice Konvenciji Vijeća Europe o zaštiti podataka – što se do danas nije dogodilo jer EU, koja nije Država članica, ne može pristupiti Konvenciji – već je to ispravljeno u "Moderniziranoj" Konvenciji Vijeća Europe za zaštitu podataka, o čemu se raspravlja u nastavku, u odlomku 1.4.3; i - prijedlog za odluku Vijeća o usvajanju akcijskog plana o sigurnosti informacija – što je dovelo do opsežne akcije na tom području od strane EU-a, uključujući i ustanovljavanje Agencije Europske unije za mrežnu i informacijsku sigurnost, ENISA, 2004. godine, te usvajanje opširne strategije informacijske- i cyber-sigurnosti, što nije dalje obuhvaćeno u ovom priručniku, ali moguće je pronaći detaljnije informacije na sljedećim poveznicama: https://www.enisa.europa.eu/about-enisa, https://ec.europa.eu/digital-single-market/en/cyber-security. Odvojene prijedloge navedene u Priopćenju Komisije (i daljnjim dokumentima koji se odnose na zakonodavnu proceduru), možete pronaći na poveznici: https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

59 Kažemo "(gotovo) u cijelosti" iz dva razloga. Prije svega, postaje sve teže, posebno u odnosu na terorizam (koncept loše definiran sam po sebi) razlikovati radnje država u odnosu na njihovu nacionalnu sigurnost od radnji koje se poduzimaju sukladno kaznenom pravu ili pravu koje se odnosi na zaštitu "međunarodne sigurnosti", "javne sigurnosti" ili "javnog reda" – pri čemu su ta pitanja sva, u manjem ili većem opsegu, sada barem djelomično podložna primjeni EU prava. Drugo, čak i ako radnje agencija država članica koje su odgovorne za nacionalnu sigurnost jesu izvan djelokruga EU prava, blisko povezane aktivnosti agencija za provedbu zakona i privatnih osoba (npr. prikupljanje i otkrivanje podataka od strane banaka sukladno zakonodavstvu o sprečavanju pranja novca, ili prikupljanje i otkrivanje evidencija o imenima putnika od strane zrakoplovnih tvrtki agencijama država članica) često su podložne primjeni EU prava (posebice prava EU-a o zaštiti podataka). Usp. drugu točku u tekstu.

60 O ograničenjima područja primjene EU-ove Opće Uredbe o zaštiti podataka, vidjeti Drugi dio, odlomak 2.3, *Ključni elementi GDPR*-a, posebno točku 2.3.1, Opće odredbe. [61] Vidjeti bilješku 67, u nastavku.

61 Vidi fusnotu 67, u nastavku.

tih direktiva, od strane tih tijela), čak i ako je *pribavljanje (dobivanje) i daljnja obrada* priopćenih podataka bila podložna drugim instrumentima (uključujući, posebice u odnosu na provedbu zakona, sve donedavno, Okvirnu odluku vijeća 2008/977/PUP i, sada, Direktivu o zaštiti podataka kod provedbe zakona iz 2016. g.), ili pak nije podložno pravu EU (ili EZ) uopće (tj. ako su to učinile nacionalne agencije za sigurnost).[62]

Treće, po samoj definiciji, direktiva se ne primjenjuje izravno na pravni poredak država članica: ona nema "izravan učinak". Naime, njene odredbe moraju se "**prenijeti**" u nacionalno pravo država članica – a kod toga, državama članicama se davalo (i još uvijek se daje) značajno **diskrecijsko pravo**. To je svakako bio slučaj u odnosu na dvije direktive o kojima se raspravlja u nastavku – te, kako će biti izneseno u Drugom dijelu, to je dovelo do značajnih odstupanja (različitosti) između nacionalnih prava država članica koje su preuzele ("prenijeti") te direktive; to je doista bio jedan od glavnih razloga za odabir forme (izravno primjenjive) uredbe kao nasljednika Direktive o zaštiti podataka iz 1995. g., točnije GDPR-a (premda, kako ćemo vidjeti u tom dijelu, Uredba i dalje također dopušta različitu primjenu u mnogo slučajeva.[63]

1.3.2 Glavna Direktiva EZ-a o zaštiti podataka iz 1995. g.

OPĆENITO

Kako je navedeno ranije, ranih 1990-ih, Komisija Europskih zajednica (kako se tada zvala)[64] suočila se s dilemom. S jedne strane, zaštita podataka sve je više prepoznata kao ustavno zaštićeno pravo u EU-u, te je zahtijevala ograničenja kod korištenja i protoka osobnih podataka.[65] S druge strane, razvoj **unutarnjeg tržišta**, u tzv. "prvom stupu" Zajednice,[66]

potrebnog za slobodan protok podataka, uključujući osobne podatke, odnosio se na komercijalne transakcije. Da bi se izašlo iz ove nerješive situacije, Komisija je predložila da za ovaj prvi stup budu usvojene dvije direktive. U ovom ćemo odlomku govoriti o glavnoj direktivi, Direktivi 95/46/EZ.[67]

Cilj i svrha Direktive o zaštititi podataka iz 1995. g.:

Priznajući gore spomenutu dilemu, Europska zajednica je dodijelila direktivi dva povezana cilja: osiguravanje **visokog stupnja zaštite podataka** širom tadašnjeg "prvog stupa" Zajednice, kao svojevrsnog *conditio sine*

---

62 O sličnim pitanjima koja su se javila u odnosu na EU-ovu Opću uredbu o zaštiti podataka, pogledati Drugi dio, posebno odlomak 2.2, Status i pristup GDPR-a: harmonizacija Status i pristup GDPR-u: izravna primjena uz posebne klauzule.

63 Pogledati Drugi dio, posebno odlomak 2.2, Status i pristup GDPR-a: harmonizacija uz fleksibilnost.

64 Pogledati bilješku (fusnotu) 67, u nastavku.

65 Zaštita podataka se sada izrijekom priznaje kao sui generis pravo u Članku 8. Povelje Europske unije o temeljnim pravima (CFR), za razliku od (premda naravno blisko povezano sa) pravom na privatni i obiteljski život i privatnost, zaštite iz Članka 7. CFR je proglašena tek 2000.g., ali nije dobila puni pravni učinak sve do stupanja na snagu Ugovora iz Lisabona na dan 1. prosinca 2009.g. Pogledati: https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union (HR: https://hr.wikipedia.org/wiki/Povelja_Europske_unije_o_temeljnim_pravima) Drugim riječima, Povelja nije još imala punu pravnu snagu u vrijeme kad su direktive predložene. Međutim, čak i prije nego li je Povelja izrađena ili prije nego li je dobila pravne učinke, temeljna prava su već dobila kvaziustavan status u Europskim zajednicama, Pogledati: Francesca Ferraro and Jesús Carmona, Fundamental Rights in the European Union – The role of the Charter after the Lisbon Treaty (Temeljna prava u Europskoj uniji – Uloga Povelje nakon Ugovora iz Lisabona), European Parliament Research Service, Brussels, ožujak 2015, odlomak 2: EU Fundamental rights prior to the Lisbon Treaty, dostupno (ENG) na: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf Tvorci Direktive o zaštiti podataka iz 1995.g. stoga su s pravom uvrstili zaštitu osobnih podataka kao temeljno pravo u osnovi predloženog instrumenta

66 Ugovor o Europskoj uniji, potpisan u Maastrichtu na dan 7. veljače 1992. g. ("Ugovor iz Maastrichta"), donio je strukturu s tri stupa pod jednim krovom. Prvi stup se sastojao od izvorne Europske ekonomske zajednice – *the European Economic Community* (EEZ - EEC), Europske zajednice za ugljen i čelik – *the European Coal and Steel Community* (EZUČ - ECSC) i Europske zajednice za atomsku energiju – *the European Atomic Energy Community* (EZAE - EAEC) (premda je svaka od njih zadržala svoju vlastitu pravnu osobnost). Drugi i treći stup su pokrivali zajedničku vanjsku i sigurnosnu politiku - *the Common Foreign and Security Policy* (CFSP - ZVSP), odnosno suradnju na poljima pravosuđa i unutarnjih poslova - *the Justice and Home Affairs* (JHA - PUP). Stupovi su formalno ukinuti Ugovorom iz Lisabona, ali odvojeni instrumenti se i dalje izdaju za različita područja (usp. rasprava o polju primjene GDPR-a u Drugom dijelu, odlomak 2.3, u nastavku teksta). Vidjeti internetsku do stupanja na snagu Ugovora iz Lisabona 1. prosinca 2009. g. Vidjeti: https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union (HR: https://hr.wikipedia.org/wiki/Povelja_Europske_unije_o_temeljnim_pravima) Drugim riječima, Povelja nije još imala punu pravnu snagu u vrijeme kad su direktive predložene. Međutim, čak i prije negoli je Povelja izrađena ili prije negoli je dobila pravne učinke, temeljna prava su već dobila kvaziustavan status u Europskim zajednicama, Vidjeti: Francesca Ferraro and Jesús Carmona, Fundamental Rights in the European Union – The role of the Charter after the Lisbon Treaty (Temeljna prava u Europskoj uniji – Uloga Povelje nakon Ugovora iz Lisabona), European Parliament Research Service, Brussels, ožujak 2015, odlomak 2: *EU Fundamental rights prior to the Lisbon Treaty*, dostupno (ENG) na: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf Tvorci Direktive o zaštiti podataka iz 1995. g. stoga su s pravom uvrstili zaštitu osobnih podataka kao temeljno pravo u osnovi predloženog instrumenta.

67 Puni naziv: *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka), SL L281, 23.11.1995, str. 31–50, dostupno na (HR): https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:31995L0046&from=en

qua non za **slobodan protok osobnih podataka** u okviru glavnog elementa stupa, **unutarnjeg tržišta**, tada tek u nastajanju (vidjeti članak 1 Direktive i Uvodnu izjavu br. 10, a posebno 11).

Ključne značajke Direktive o zaštiti podataka iz 1995. g.:

U nastavku su **ključne značajke** Direktive o zaštiti podataka iz 1995. g., usporedno s Konvencijom iz 1981. g. (Naglašavamo: Nova svojstva ili značajke koje sadrže važne nove elemente označene su oznakom - iako treba napomenuti da se oni često oslanjaju na sugestije koje su već napravljene ili navode u uvodnim izjavama Konvencije). Opis tih ključnih obilježja Direktive iz 1995. ima za cilj pružiti pregled nekih temeljnih komponenti pristupa zaštite podataka u EU-u, koji su u cijelosti ponovno potvrđeni u Općoj uredbi o zaštiti podataka iz 2016. te su u skladu s tim objašnjeni ovdje, glavne nove značajke uvedene putem Uredbe bit će istaknute u drugom dijelu. Najvažnije novine bile su zahtjevi neovisnih tijela za zaštitu podataka te mjere kojima se osigurava kontinuirana zaštita podataka prenesenih u treće zemlje (zemlje koje nisu članice Europske unije ni dio Europskog gospodarskog prostora).

Definicije:

Direktiva je proširila temeljne **definicije** Konvencije iz 1981. g. i dodala nove. Posebice, razjasnila je (unutar definicije "osobnih podataka") gdje se pojedinci trebaju smatrati kao osobe "čiji se identitet može utvrditi" (od strane "bilo koga") i (u odvojenoj definiciji) kada se ručno obrađeni skup podataka treba smatrati dostatno "***strukturiranim***" da bi se na njega primijenila Direktiva. "[Strukturirana] ručno obrađena dokumentacija" uključena je u područje primjene Direktive da bi se izbjeglo zaobilaženje njenih pravila korištenjem takve dokumentacije.

Direktiva je donijela ***ponešto modificiranu definiciju "voditelja obrade"***, te je dodala ***sveobuhvatnu definiciju "obrade osobnih podataka"*** i definicije koncepata **izvršitelja obrade**, "***treće stranke***" i "***primatelja***". Također je dodala definiciju "***suglasnosti osobe čiji se podaci obrađuju***" koja je u praksi izložila uvjete koji trebaju biti zadovoljeni prije nego se bilo kakva navodna suglasnost može smatrati valjanom: suglasnost, da bi bila valjana, morala je biti "***dobrovoljno dana, posebna i informirana***" i na neki način ***izražena izjava volje*** (čl. 2(h)).[68]

Dok je Konvencija iz 1981. g. imala četiri definicije, Direktiva ih je donijela osam (ili devet, ako se računa definicija "osobe koju se može utvrditi" u okviru definicije "osobnih podataka" kao jedna odvojena).

Načela zaštite podataka:

Direktiva je u velikom dijelu ponovila **načela zaštite podataka** iz Konvencije iz 1981. g., ali s nekim **pojašnjenjima**, uključujući da ***svrha*** u koju se osobni podaci obrađuju ne bi trebala biti samo "*posebna*" i "*zakonita*" (kako je već propisano u članku 5(b) Konvencije), već također i "*izričita*" (čl. 6(1)(b)), te u mjeri u kojoj se tiče "*[daljnje obrade podataka u povijesne, statističke ili znanstvene svrhe]*" (vidjeti čl. 6(1)(c) i (e)).

ZAKONSKA OSNOVA ZA OBRADU PODATAKA

Glavna nova značajka Direktive iz 1995. bila je da je, kako bi se postigla veća usklađenost između zakona država članica, u članku 7. **utvrđen iscrpan popis "mjerila (kriterija) za zakonitost obrade podataka"** – koji su kasnije nazvani **"pravna osnova"** za obradu osobnih podataka. Prema Direktivi, obrada osobnih podataka (koji nisu osjetljivi) bilo je dopuštena samo ako (ukratko): je osoba čiji se podaci obrađuju ***nedvosmisleno*** dala svoju **suglasnost** (koja naravno također mora biti "***dobrovoljno dana, posebna i informirana***" i ***izražena***: ll. 2(h), navedeno ranije u tekstu); ili

(a) obrada je bila ***potrebna*** za izvršenje **ugovora u** kojem je osoba čiji se podaci obrađuju stranka ili kako bi se poduzele mjere na zahtjev osobe čiji se podaci obrađuju prije sklapanja ugovora (npr. za provjeru kreditne sposobnosti); ili

68 Suglasnost je moralo biti u obliku "dobrovoljno dana, posebna i informirana **izjava volje, kojom osoba čiji se podaci obrađuju daje svoju suglasnost** da se obrade osobni podaci koji se na nju odnose", da citiramo cjelovit tekst.

(b) obrada je ***potrebna*** za sukladnost sa **zakonskom obvezom** kojoj voditelj obrade podliježe; ili

(c) obrada je ***potrebna*** kako bi se zaštitili **vitalni interesi osobe čiji se podaci obrađuju**; ili

(d) obrada je **potrebna** za izvršavanje **zadatka koji se provodi zbog javnog interesa ili pri izvršavanju javne ovlasti** koju ima voditelj obrade ili treća stranka kojoj se podaci otkrivaju; ili

(e) obrada je **nužna** u svrhe **zakonitog interesa** kojeg ima voditelj obrade ili treća stranka ili stranke kojima se podaci otkrivaju, osim kada su ti podaci podređeni interesu ili temeljnim pravima i slobodama osobe čiji se podaci obrađuju koja zahtijeva zaštitu na temelju članka 1(1) [tzv. "zakoniti interesi" ili kriterij "ravnoteže"/pravna osnova].

Jednostavno rečeno: u većini slučajeva obrada neosjetljivih osobnih podataka bila je dopuštena, bilo na temelju zakona, ili ugovora, ili uz pristanak nositelja podataka, ili na temelju toga da je služila legitimnom/zakonitom interesu voditelja koji nije bio izvagan u odnosu na interes ili temeljna prava i slobode ispitanika.

Popis ovakve vrste nije bio sadržan u Konvenciji o zaštiti podataka iz 1981. godine.

Posebna pravila kod obrade osjetljivih podataka

Direktiva iz 1995. g. navela je uglavnom iste **glavne** "**posebne vrste podataka**" – koji se obično nazivaju "**osjetljivi podaci**" – kako su navedeni i u Konvenciji iz 1981. g., s manjim izmjenama, tj.:[69]

> podaci kojima se otkriva rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i … podataka u vezi sa zdravljem ili spolnim životom

Međutim, umjesto da samo propiše da se takvi podaci "*ne mogu automatizirano obrađivati ako nacionalno pravo ne predviđa odgovarajuću zaštitu*" (Konvencija Vijeća Europe, čl. 6), Direktiva u članku 8(1), propisuje **načelnu zabranu** obrade takvih osjetljivih podataka, uz primjenu ograničenog broja **iznimaka**. Glavne iznimke u biti su se svodile na **posebno restriktivne pravne osnove** za obradu osjetljivih podataka. To su bili (ponovo ukratko):

- obrada po osnovi ne samo dobrovoljne, posebne i informirane, već također i ***izričite* suglasnosti** osobe čiji se podaci obrađuju, osim kada bi nacionalno zakonodavstvo države članice zabranjivalo obradu takvih podataka čak i ako osoba čiji se podaci obrađuju da svoju suglasnost u posebnim okolnostima (čl. 8(2)(a));
- obrada koja je ***potrebna*** u svrhu izvršavanja obveza i prava voditelja obrade na području **zakonodavstva u zapošljavanju** (pod uvjetom da nacionalno zakonodavstvo pruža "odgovarajuću zaštitu") (čl. 8(2)(b));
- obrada koja je **potrebna** radi zaštite **vitalnih interesa** osobe čiji se podaci obrađuju ili druge osobe kada osoba čiji se podaci obrađuju nije fizički ili pravno sposobna dati svoju suglasnost (čl. 8(2)(c));
- obrada koju "provodi tijekom svojih zakonitih aktivnosti uz odgovarajuću zaštitu ustanova, udruga ili neko drugo **neprofitno tijelo s političkim, filozofskim, vjerskim ili sindikalnim ciljem** i pod uvjetom da se obrada odnosi jedino na članove tijela ili na ***osobe koje su u redovitom kontaktu*** s njime u pogledu njihove svrhe te da se podaci ***ne otkrivaju trećoj stranci*** bez suglasnosti osobe čiji se podaci obrađuju" (čl. 8(2)(d));
- obrada (osjetljivih) osobnih podataka "**koje je objavila osoba čiji se podaci obrađuju**" (čl. 8(2)(e), prva rečenica); i
- obradu (osjetljivih) osobnih podataka kada je to "potrebno radi uspostave, provedbe ili obrane **pravnih zahtjeva**" (čl. 8(2)(e), druga rečenica).

69 Konvencija iz 1981. g. nije uključila reference na "etničke" podatke, referencu na "religijska ili druga uvjerenja" (a ne "vjerska ili filozofska uvjerenja"), te nije uključila članstvo u sindikatu.

Posebice, popis nije uključivao "**legitimne interese**" ni kriterij "**ravnoteže**": obrada osjetljivih podataka ne bi mogla, već po osnovi Direktive, *načelno* biti provedena u svrhe legitimnih interesa voditelja obrade ili treće stranke, koji nisu podređeni interesu zaštite temeljnih prava osobe čiji se podaci obrađuju.

Međutim, Direktiva je također propisivala da u načelu zabrana obrade osjetljivih podataka (pazite: bilo koje vrste osjetljivih podataka) nije bila primjenjiva "*kada je obrada podataka **potrebna** u svrhe **preventivne medicine, medicinske dijagnoze**, zdravstvene **skrbi** ili **liječenja** ili **upravljanja zdravstvenim službama***", pod uvjetom da to podliježe dotičnoj obvezi čuvanja tajne (čl. 8(3)). Primijetite da se ovo primjenjuje na bilo koju vrstu osjetljivih podataka – ali, naravno, takvi podaci mogu se i dalje koristiti samo za takve svrhe kada je to relevantno (npr. informacije o rasnom podrijetlu mogu biti relevantne u odnosu na određene bolesti,

kao što je anemija srpastih stanica; a religijska uvjerenja osobe mogu biti relevantna za određeno liječenje, kao što je transfuzija krvi u slučaju Jehovinih svjedoka).

Štoviše, premda su gore navedena pravila kao takva bila stroga, Direktiva je također sadržavala mnogo općenitiju odredbu (čl. 8(4)) koja je dopuštala državama članicama da mogu propisati **dodatne iznimke** – tj. dopustiit obradu (bilo koje vrste) osjetljivih podataka osim onih po osnovi navedenoga u članku 8(2) – bilo zakonom ili odlukom svojeg nadzornog tijela (tijelo za zaštitu podataka, "***zbog značajnog javnog interesa***", pod uvjetom da je to učinjeno uz utvrđivanje "***odgovarajuće zaštite***" – što će definirati država članica.

Direktiva je također propisala ponešto restriktivniji pristup obradi **osobnih podataka koji se odnose na kaznene presude** (čl. 8(5)) i obradu **nacionalnih identifikacijskih brojeva ili drugog načina "identifikacije za opću uporabu"** (čl. 8(7)) – ali je ostavila detaljnije reguliranje takve obrade državama članicama.

Slično tome, premda je bila jasnija negoli Konvencija iz 1981. oko potrebe **usklađivanja (uravnoteženja) zaštite podataka i slobode izražavanja i informacija**, ostavila je specifično postizanje ove ravnoteže također državama članicama (čl. 9).

Obavještavanje osoba čiji se podaci obrađuju

Konvencija o zaštiti podataka iz 1981. g. tražila je samo neku opću transparentnost oko "*postojanja automatizirane zbirke osobnih podataka, njezinoj glavnoj svrsi, te identitetom i uobičajenim boravištem ili sjedištem upravitelja zbirke*" (čl. 8(a)).

Nasuprot tome, članci 10 i 11 iz Direktive o zaštiti podataka iz 1995. g. donose donekle detaljnije **podatke koje treba pružiti bilo koji voditelj obrade osobama čiji se podaci obrađuju**, *na vlastitu inicijativu voditelja obrade*, kada su, u odnosnom slučaju, osobni podaci prikupljeni od tih osoba ili od treće stranke. Pojedinosti koje se trebaju pružiti uključivale su, u oba slučaja, ***identitet voditelja obrade*** i ***svrhe obrade podataka***. ***Daljnji podaci*** (uključujući podatke o tome jesu li podaci koji se prikupljaju obvezni ili ne, podaci o bilo kojem otkrivanju podataka) morali su biti dani kao nužni da bi se osigurala poštena obrada (vidjeti čl. 10(c) i 11(1)(c)).

Prava osobe čiji se podaci obrađuju

Konvencija o zaštiti podataka iz 1981. g. već je tražila da ispitanici trebaju imati pravo **pristupa** svojim podacima na zahtjev, u primjerenim vremenskim rokovima; pravo na **ispravak ili brisanje** podataka koji su bili netočni ili obrađeni protivno načelima zaštite podataka; i pravo na **pravni lijek** ako nije bilo poštivano ostvarenje ovih prava (čl. 8(b) – (d)).

Direktiva je potvrdila prva dva prava, ali je dodala i **važan daljnji detalj**. Potvrdila je da **pravo na pristup podacima** uključuje pravo da podaci budu "priopćeni" osobi čiji se podaci obrađuju (što je već bilo predviđeno Konvencijom), ali je dodala da ovo mora biti učinjeno "*u razumljivom obliku*" i da također treba dostaviti i "*bilo koje podatke o njihovom **izvoru** [izvoru podataka]*" (čl. 12(a), druga natuknica). Dodano je "***blokiranje***

(podataka)" kao opcija pored ispravka ili brisanja (premda bez definiranja samog tog koncepta)[70] (čl. 12(b)); te je odredila da ***trećim strankama*** kojima su podaci bili otkriveni (čl. 12(c)) treba skrenuti pažnju na bilo koje ispravke, blokiranja ili brisanja.

Također je uvela nova prava: **opće pravo na prigovor** na obradu "zbog jakih i zakonitih razloga", "barem" u odnosu na obradu radi izvršavanja zadatka koji se provode zbog javnog interesa ili pri izvršavanju javne ovlasti, ili se temelje na "zakonitom interesu"/kriteriju "ravnoteže" – pri čemu se takav prigovor mora usvojiti ako je bio "osnovan" (čl. 14(a)); određenije i jače **pravo prigovora na obradu podataka u svrhe izravnog marketinga** (u to doba, uglavnom putem izravne pošte – to je doba prije interneta i "spam" elektronske pošte) – koje se uvijek mora poštivati, bez potrebe da osoba čiji se podaci obrađuju pruži bilo kakvo obrazloženje za isto (čl. 14(b)); te **pravo osobe čiji se podaci obrađuju da ne bude podložna odluci koja je osnovana na automatskoj obradi podataka koja se temelji na izradi profila**[71] koja je proizvela pravne ili druge značajne učinke (uz primjenu važnih, ali strogo kvalificiranih ***iznimaka***) (čl. 15). U tom pogledu, važno je primijetiti da članak 12(a), treća natuknica, navodi da osobe čiji se podaci obrađuju također imaju **novo** pravo dobiti (u kontekstu zahtjeva za pristupom) **informaciju o "logici"** uključenoj u bilo koju automatsku obradu podataka koji se tiču nje, "barem" u slučaju u cijelosti automatskih odluka koje se temelje na izradi profila. Ova prava iz Direktive 1995, koja su prenesena i dodatno ojačana kroz GDPR, postaju sve značajnija pri donošenju odluka temeljenih na umjetnoj inteligenciji. S obzirom na umjetnu inteligenciju, ovo postaje još važnije.

Povjerljivost i sigurnost podataka

Konvencija iz 1981. je samo propisivala da "prikladne sigurnosne mjere" trebaju biti poduzete za zaštitu osobnih podataka protiv "slučajnog ili neovlaštenog uništenja ili slučajnog gubitka, kao i protiv neovlaštenog pristupa, izmjene ili otkrivanja" (čl. 7).

Direktiva je značajno proširila postojeće rješenje namećući, prije svega, **obveza povjerljivosti** svakoj osobi koja sudjeluje u obradi osobnih podataka (čl. 16), a potom propisujući da se traži od voditelja obrade da provede "*odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke od slučajnog ili nezakonitog uništavanja ili slučajnoga gubitka, izmjene, neovlaštenog otkrivanja ili pristupa, posebno kada obrada uključuje prijenos podataka putem mreže te protiv svih drugih nezakonitih oblika obrade*" (čl. 17(1), s daljnjim pojedinostima). Ova potonja odredba preuzeta je iz saveznog njemačkog Zakona o zaštiti podataka iz 1977. g.

Također je propisala važne nove zahtjeve u slučaju kada voditelja obrade izabere obrađivača da obrađuje podatke za njegov (račun voditelja obrade), uključujući uvjet "*dovoljnih jamstava*" u pogledu sigurnosti i povjerljivosti, te uvjet detaljnog pisanog ugovora sklopljenog između voditelja obrade i izvršitelja obrade (čl. 17(2) – (4)).

Ograničenja kod prekograničnog protoka podataka

Kako je navedeno u odlomku 1.2.3, ranije u tekstu, Konvencija iz 1981., u izvornom obliku kako je usvojena, nije tražila od država članica da usvoje **zabranu iznošenja osobnih podataka sa svojeg teritorija u državu koja nije pružala sličnu zaštitu.** Bavila se jedino protokom osobnih podataka između država stranaka konvencije. Uvođenje takve zabrane (uz primjenu ograničenih iznimki) bilo je stoga nova važna značajka Direktive iz 1995. g.

---

70 Odgovarajući koncept "**ograničavanje obrade**" definiran je u GDPR-u kao "*označivanje pohranjenih osobnih podataka kako bi se ograničavanje njihove obrade u budućnosti*" (čl. 4(3) GDPR-a).

71 U cijelosti: "odluku koja proizvodi pravne učinke u vezi nje [osobe čiji se podaci obrađuju] ili na nju značajno utječe i koja je isključivo osnovana na automatskoj obradi podataka s namjerom procjene određenih osobnih vidova koji se na nju odnose, kao što je njezin uspjeh na poslu, kreditna sposobnost, pouzdanost, ponašanje itd." Ova je odredba preuzeta izravno iz francuskog Zakona o zaštiti podataka iz 1978. g., čl. 2. i 3.

Posebice, propisivala je da osobni podaci na koje se primjenjuje Direktiva mogu u načelu biti preneseni jedino u treće zemlje koje osiguravaju razinu zaštite koja bi se mogla smatrati "**odgovarajućom**" u smislu Direktive (čl. 25(1)); te da će Europska komisija trebati utvrditi (pomoću onoga što je postalo poznato kao "***odluka o primjerenosti***" razine zaštite) je li to slučaj u odnosu prema specifičnoj trećoj zemlji (čl. 25(2)).[72] Komisija je nastavila utvrđivati "odgovarajuću razinu zaštite" ne samo u odnosu na treće zemlje u cjelini, već također u odnosu na **sektore** u pojedinim zemljama (npr. inicijalno, režim za tijela javnog sektora u Kanadi) i doista za posebne **sheme** ustanovljene u određenim državama (npr. "*Safe Harbor*" pravilo (pravilo sigurne luke) ustanovljen u SAD-u, tada zamijenjen pravilom "Štita *privatnosti*"/"*Privacy Shield*").

Načelna zabrana prijenosa u zemlje (ili sektore u zemljama) bez odgovarajuće zaštite podlijegala je ograničenom broju **iznimaka** navedenih u članku 26(1) Direktive, većina kojih je bila slična pravnim osnovama za obradu općenito, tj. (ukratko):

(a) osoba čiji se podaci obrađuju dala je svoju ***nedvosmislenu* suglasnost** predloženom prijenosu (koja je, naravno, također morala biti "***dobrovoljna, posebna i informirana***" te ***izražena***: čl. 2(h), opisano ranije u tekstu);

(b) da je prijenos bio **potreban** radi izvršenja **ugovora** između osobe čiji se podaci obrađuju i voditelja obrade ili provedbe predugovornih mjera poduzetih na zahtjev osobe čiji se podaci obrađuju (npr. provjera kreditne sposobnosti);

(c) prijenos je bio **potreban** za sklapanje ili izvršenje **ugovora** sklopljenog u interesu osobe čiji se podaci obrađuju između voditelja obrade i treće stranke (npr. hotelska rezervacija);

(d) prijenos je ***potreban*** ili ***propisan zakonom*** radi **važnog javnog interesa** ili uspostave, izvršenja ili obrane **pravnih zahtjeva**;

(e) prijenos je ***potreban*** kako bi se zaštitili **vitalni interesi osobe čiji se podaci obrađuju**; ili

(f) prijenos se obavlja iz **evidencije koja je na raspolaganju javnosti** (uz primjenu bilo kojih uvjeta koji općenito vrijede za pristup toj evidenciji).

Osim toga, države članice su smjele **dopustiti** prijenose u slučajevima u kojima je voditelj obrade poduzeo "***odgovarajuće zaštitne mjere***" kako bi zaštitio pravo na zaštitu osobnih podataka pojedinaca čiji se podaci obrađuju (čl. 26(2)) – npr., u obliku ***ad hoc odredbi o prijenosu podataka*** ili (za prijenose podataka unutar društva) pomoću tzv. "***Binding Corporate Rules*"/"Obvezujućih korporativnih pravila"** (OKP-ovi); a Komisija je bila **ovlaštena** odobriti određene "***standardne ugovorne klauzule***" za prijenose podataka, što bi osiguralo takvu zaštitu (čl. 26(4)).

Određeni broj TZP-a (tijela za zaštitu osobnih podataka), i po njihovom mišljenju, RS29, također su razmatrali zaštitne mjere sadržane u tzv. obvezujućim korporativnim pravilima (OKP), tj. u pravilima koja su sastavila međunarodna poduzeća ili grupe tvrtki koje su regulirale interne upotrebe i tokove osobnih podataka unutar takvih tvrtki ili grupa. Unatoč oklijevanju nekih drugih TZP-a, ideja je formalno bila uključena u GDPR (kao što je navedeno u drugom dijelu).

Ograničenja u vezi s prijenosom osobnih podataka u treće zemlje bez odgovarajuće zaštite potaknula su djelovanje izvan Europe. Posebno, španjolski i francuski TZP iskoristili su ga za promicanje usvajanja odgovarajućih zakona u svojim globalnim jezičnim zonama, tj. u Latinskoj Americi i zemljama francuskog govornog područja, posebno u Africi.

NB: Kako je opisano pod točkom 1.2.3, ranije u tekstu, uvjet "odgovarajuće razine zaštite" za prijenose podataka uveden je za Konvenciju iz 1981. g. u Dodatnom protokolu uz tu Konvenciju iz 2001., s ciljem usklađivanja režima Konvencije u tom pogledu s režimom iz Direktive EZ-a iz 1995. g. (vidjeti čl. 2(1) Protokola)

72 Izraz "odgovarajuća zaštita" bio je odabran zbog toga što je izraz "ekvivalentna" bio rezerviran u pravu EZ-a (tadašnjeg EU-a) vezano za odnose između pravila među državama članicama dok se, po osnovi međunarodnog prava, radilo o "ekvivalentnom učinku". Ali, u svojoj presudi u predmetu *Maximillian Schrems v. Data Protection Commissioner*, presuda SEU-a u predmetu C-362/14, 6. prosinca 2015. g., Sud je zauzeo stav da izraz "odgovarajuća zaštita" treba biti tumačen kao da se u biti traži "u bitnome ekvivalentna" zaštita u trećoj državi: vidjeti st. 96 presude – ali to je, naravno, bilo mnogo godina nakon što je usvojena Direktiva iz 1995. g. (a pogotovo Dodatni protokol iz 2001. g. uz Konvenciju iz 1981. g., opisano kasnije u tekstu).

– premda se to jasno primjenjuje samo na one države članice izvorne Konvencije koje su također prihvatile i Protokol.[73]

Međutim, nejasno je može li se, odnosno smije li se, izraz "odgovarajuću razinu zaštite" iz ovog članka Protokola, tumačiti sukladno presudi u slučaju *Schrems*[74]- te je stoga nejasno je li Protokol zapravo postigao ovaj cilj.

Pravila ponašanja/kodeksi (i potvrde/certifikati)

Još jedna nova značajka koju je uvela Direktiva bilo je njeno pozivanje na **pravila ponašanja** "*koja imaju za cilj doprinijeti ispravnoj provedbi nacionalnih propisa koje donesu države članice u skladu s ovom Direktivom, uzimajući u obzir posebne značajke različitih područja*" (čl. 27(1)) – premda je doseg ovoga bio samo "poticanje" takvih kodeksa (*idem*); traženje od država članica da predvide procjenu ***prijedloga nacionalnih pravila*** (čl. 27(2)); i sama predviđajući Radnu skupinu iz članka 29. (RS29, o kojoj se govori u nastavku pod tim naslovom) da na sličan način procijeni ***nacrt prijedloga kodeksa na razini Zajednice*** (čl. 27(3)).

U praksi je tek nekolicina takvih kodeksa pravila odobrena ili čak predana na odobrenje. Prvi nacrt kodifikacije pravila Europske federacije direktnog i interaktivnog marketinga (*the European direct marketing association*) (FEDMA), Europski kodeks pravila za korištenje osobnih podataka u izravnom marketingu predan je RS29 godine 1998. g., ali je konačna verzija odobrena tek 2003. godine.[75] Nacrt Kodeksa pravila ponašanja za pružatelje *cloud* usluga, sastavljen od strane sektorske radne grupe osnovane 2013. godine, kojom zajednički predsjedavaju dvije Glavne uprave EU-a (GU za komunikacijske mreže, sadržaje i tehnologije - *DG connect* i GU za pravosuđe i potrošače - *DG Just*) predan je RS29 u siječnju 2015. godine, ali ga RS29 nije odobrio u svojem mišljenju o nacrtu; stoga ostaje u fazi "radovi u tijeku".[76]

Iako nije izrijekom spomenuto u Direktivi, Europska komisija je također poticala osnivanje shema certificiranja.[77] Pružila je početno financiranje grupi TZP-ova i stručnjacima koje vodi Schleswig-Holstein TZP za osnivanje **paneuropske sheme certificiranja, Europski "pečat privatnosti" (the *European Privacy Seal*), tj. EuroPriSe**, pod kojim se proizvodi i usluge koje uključuju korištenje osobnih podataka mogu procijeniti i, ako se ocijeni da su sukladni Direktivi (a kada je to primjenjivo, i drugim EU instrumentima o zaštiti podataka, kao što je Direktiva o e-privatnosti, o čemu se govori pod sljedećim naslovom), odobrava im se potvrda (certifikat) koji potvrđuje takvu sukladnost (premda, s obzirom da u Direktivi 1995 ne postoji formalna obveza za tu shemu, te potvrde naravno ne bi imale pravni učinak).[78]

Pravila o "važećem (mjerodavnom) pravu"

Kako bi trebalo jasno slijediti iz različitih tekstova pod različitim ranijim naslovima, države članice su prema Direktivi imale značajno diskrecijsko pravo kod određivanje točnog načina na koji one žele "transponirati" odredbe Direktive; mnoge od tih odredbi prepustile su državama članicama da usvoje takva pravila kakva smatraju odgovarajućima u određenim kontekstima. To je dovelo do ozbiljnog manjka usklađenosti[79] – što

---

73 Vidjeti bilješku (fusnotu) 45, prethodno u tekstu.

74 Vidjeti bilješku (fusnotu) 68, ranije u tekstu.

75 Tekst Kodeksa (pravila ponašanja): https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf
Članak 29. Radna skupina Mišljenje (Opinion) 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, kojim se podržava kodeks (RS77, usvojeno 13. lipnja 2003. g.), dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf

76 Vidjeti: https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(19. srpanj 2013. g. - općenita pozadina i dokumenti koji su služili kao osnova) https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers (12. listopad 2015. g. – najnovije dostupne informacije)
Članak 29. Radna skupina, Mišljenje (Opinion) 02/2015 on C-SIG Code of Conduct on Cloud Computing (RS232, usvojeno 22. rujna 2015. g.), dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

77 Kada se internet počeo širiti diljem svijeta ranih 1990-ih, francusko nadzorno tijelo za zaštitu podataka je predložilo drugim tijelima za zaštitu podataka u EU i Europskoj komisiji da sheme certificiranja mogu biti vrlo korisna sredstva za rješavanje online usluga utemeljenih izvan Europe, ali ništa nije učinjeno po tom pitanju u to vrijeme.

78 Kada se internet počeo širiti diljem svijeta ranih 1990-ih, francusko nadzorno tijelo za zaštitu podataka je predložilo drugim tijelima za zaštitu podataka u EU i Europskoj komisiji da sheme certificiranja mogu biti vrlo korisna sredstva za rješavanje online usluga utemeljenih izvan Europe, ali ništa nije učinjeno po tom pitanju u to vrijeme.

79 Vidjeti studiju koju je naručila EU, autora Douwe Korffa, Report on an EU study on the implementation of the [1995] data protection directive (Izvješće o EU studiji o primjeni directive o zaštiti podataka iz 1995. g.), 2002, dostupno na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667

je bio jedan od glavnih razloga zašto je odabrana forma uredbe za instrumente koji su naslijedili Direktivu.[80]

Poteškoće izazvane ovim odstupanjima bile su u nekoj mjeri ublažene ključnom odredbom iz Direktive o zaštiti podataka iz 1995. g., odredbom o "važećem (mjerodavnom) pravu". Ova odredba (čl. 4) učinkovito je predvidjela tri različita pravila za privatni sektor:

(1) voditelji obrade koji imaju poslovni nastan na području samo jedne države članice moraju primijeniti nacionalne propise o zaštiti podataka te države članice u odnosu na bilo koju obradu koju nadziru i koju "provode u smislu aktivnosti poslovnog nastana [tog] voditelja obrade" (čl. 4(1)(a), prva rečenica);

(2) voditelji obrade koji imaju poslovni nastan na području nekoliko država članica [to znači: imaju poslovni nastan u više od jedne države članice] moraju osigurati "da svaki od tih poslovnih nastana ispunjava obveze propisane važećim nacionalnim pravom" (što ne mora biti država osnivanja dotičnog poslovnog nastana) (čl. 4(1)(a), druga rečenica);

(3) voditelji obrade koji nisu osnovani u Zajednici (EU) moraju primijeniti pravo bilo koje države članice na čijem teritoriju "su koristili opremu, bilo da je automatizirana ili ne", (čl. 4(12)(c)); i takvi voditelji obrade moraju "imenovati zastupnika" na tom teritoriju (čl. 4(2)).[81]

Bitno je primijetiti da pod sva ova tri pravila, **podaci o svim pojedincima** ("fizičke osobe") koje obrađuju dotični voditelji obrade moraju biti zaštićeni, ***neovisno o tome jesu li osobe*** čiji se podaci obrađuju u EU-u ili ne, te neovisno o tome jesu li državljani EU-a ili rezidenti ili ne – sukladno načelu *univerzalnosti ljudskih prava*.[82]

Ta je pravila bilo teško primijeniti u praksi (posebice u odnosu na voditelje obrade koji nemaju poslovni nastan u EU/EGP-u),[83] ali su pružila barem neke smjernice o tome kako postupati s različitim zakonima u različitim državama članicama koji bi se u teoriji mogli primijeniti na bilo koju aktivnost transnacionalne obrade osobnih podataka. Ni jedna takva odredba koja je ciljala na izbjegavanje "sukoba zakona" nije bila sadržana u Konvenciji o zaštiti podataka iz 1981. g.

Što se tiče javnog sektora, određivanje primjenjivog prava u praksi je bilo mnogo izravnije: sva javna tijela, uključujući diplomatske institucije (diplomatska predstavništva), bila su podložna isključivo zakonu o zaštiti podataka (ili zakonima) njihovih država članica.

Nadzorna tijela

Još jedna velika novost u Direktivi iz 1995. g., u usporedbi s Konvencijom iz 1981. g.,[84] bio je zahtjev da sve države članice moraju imenovati

> jedno ili više javnih tijela na njenom području odgovorno za nadzor primjene odredbi koje su donijele države članice u skladu s ovom Direktivom (čl. 28(1), prva rečenica).

Ova "**nadzorna tijela**" – u praksi češće zvana ***tijela za zaštitu podataka*** ili ***TZP-ovi*** – (od kojih je nekoliko bilo u saveznim državama članicama), morala su dobiti široke ***istražne ovlasti***, ***ovlasti za posredovanje*** i ***usmjeravanje*** (uključujući ovlasti naređivanja blokiranja, brisanja ili uništavanja podataka, ili zabrane obrade)

80 Vidjeti Drugi dio, odlomak 2.1 kao i tekst pod prvim podnaslovom, "*Uredba …*" u odlomku 2.2, u nastavku teksta.

81 Primjena ovog trećeg pravila bila je komplicirana zbog korištenja različitih riječi (termina) u raznim jezičnim verzijama: engleski tekst je navodio korištenje "equipment" u svrhe prijenosa preko teritorija Zajednice, dok su druge (naravno, jednako autentične) verzije govorile o "sredstvima" (F: moyens; D: Mittel). To je dovelo do toga da je Ujedinjeno Kraljevstvo ograničilo primjenu ovog pravila na situacije u kojima voditelj obrade izvan EU/EGP ima u vlasništvu opremu u EU/EGP-u (u slučaju, u UK), dok su druge države smatrale da je i sama prisutnost smart (pametnog) telefona u EU/EGP-u dostatna da time predstavlja "korištenje" od strane voditelja obrade takvog uređaja za prijenos podataka, što podliježe primjeni Direktive.

82 Vidjeti Douwe Korff, Maintaining Trust in a Digital Connected Society (Očuvanje povjerenja u digitalno povezanom društvu), izvješće napisano za Međunarodnu telekomunikacijsku uniju (the International Telecommunications Union, ITU), svibanj 2016. g., odlomak 2.3, *Universality of human rights (Univerzalnost ljudskih prava)*, dostupno ovdje: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf

83 Vidjeti: Douwe Korff, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"*, u: Recht der Datenverarbeitung, Year 10 (1994), Vol. br. 5- 6, p. 209 ff; *The question of "applicable law" (Pitanje "mjerodavnog prava")*, u: Compliance Guide 3 – Interim report (dio novog britanskog Zakona o zaštiti podataka iz 1998 Information & Compliance Programme), Privacy Laws & Business, studeni 1999. g.

84 Već je bilo predviđeno u neobvezujućim Smjernicama UN-a usvojenima 1990. g. (vidjeti bilješku (fusnotu) 41, prethodno u tekstu). Također, kako je navedeno pod točkom 1.2.3, prethodno u tekstu, zahtjev da države osnuju neovisna nadzorna tijela po modelu bliskom smislu Direktive o zaštiti podataka iz 1995. g., uveden je za Konvenciju iz 1981. g. U Dodatnom protokolu uz tu Konvenciju iz 2001. g., s ciljem usklađivanja režima Konvencije u tom smislu s režimom iz Direktive EZ-a iz 1995. g. (vidjeti čl. 1 Protokola) – premda se to naravno primjenjuje samo na one države članice koje su stranke izvorne Konvencije, a koje su također pristupile Protokolu (kako je navedeno u bilješki (fusnoti) 45, prethodno u tekstu).

(čl. 28(3), prva i druga natuknica), te su morala biti u mogućnosti "*provedbe funkcija koje su im povjerene djelovati potpuno neovisno*" (čl. 28(1), druga rečenica). Zahtjev za neovisnošću također je uvjet demokracije i vladavine prava. Budući da zahtjevi neovisnosti nisu bili navedeni u direktivi, Komisija je morala pribjeći sudskim tužbama protiv nekoliko država članica kako bi se to pitanje razjasnilo. Rezultati tih sudskih slučajeva odražavaju se u mnogo složenijim odredbama u GDPR-u u tom pogledu.

Nadzorna tijela savjetuju tijela država članica prilikom izrade mjera ili propisa o zaštiti podataka (čl. 28(2)) i mora im biti omogućeno "sudjelovati u sudskim postupcima" u odnosu na navodna kršenja njihovih nacionalnih zakona o zaštiti podataka (čl. 28(3), treća natuknica).

Također su im stavljeni u nadležnost i obavješćivanje i "prethodna provjera", kako je objašnjeno pod sljedećim podnaslovom.

Od ključne je važnosti također da se, osim formalnijih pravnih lijekova opisanih pod sljedećim podnaslovom nakon toga, TZP-ovima moralo dati pravo "**razmatrati zahtjeve [drugim riječima: rješavati pritužbe] koje podnese bilo koja osoba**, ili bilo koja udruga koja zastupa tu osobu" vezano za pitanja zaštite podataka (čl. 28(4)).

TZP-ovi, koji surađuju na razini EU-a u "**Radnoj skupini iz članka 29**" o kojoj se govorilo pod posljednjim podnaslovom u ovom odjeljku, postali su glavni branitelji prava zaštite u vezi s obradom osobnih podataka u EU-u (čak i ako su se njihove ovlasti i učinkovitost prema nacionalnim zakonima usvojenima radi provedbe Direktive i dalje razlikovale).

Obavješćivanje i "prethodna provjera"

Obavješćivanje:

Kako bi se postigla **opća transparentnost** o obradi osobnih podataka i da bi se pomoglo osiguravanju potpunog poštivanja zakona o zaštiti podataka, Direktiva o zaštiti podataka iz 1995. g. također je predvidjela širok sustav **obavješćivanja** o aktivnostima obrade osobnih podataka (čl. 18, vidjeti čl. 19 za pojedinosti o sadržaju obavijesti); te je propisala da podaci iz obavijesti trebaju biti uneseni u **evidenciju,** koja treba biti ***dostupna javnosti*** (čl. 21(2)). Ovo se temeljilo na sustavu koji je prvi puta usvojen u Švedskoj 1973. g., a potom je preuzet u mnogim drugim državama članicama EU-a.

Međutim, Direktiva je također državama članicama dopuštala, da kao ekvivalentnu alternativu obavješćivanju, propišu ***pojednostavljenja*** ili ***iznimke*** od opće obveze obavješćivanja u (poglavito) dvije situacije, tj.:[85]

- kada su, u slučaju obrade "koja nije rizična",[86] države članice donijele "***pojednostavljene norme***" koje navode osnovne parametre za obradu (tj. svrhe obrade, podaci ili vrste podataka koji se obrađuju, kategorija ili kategorije osoba čiji podaci se obrađuju, primatelji ili vrste primatelja kojima se podaci otkrivaju, te razdoblje tijekom kojeg će se podaci čuvati)(čl. 18(2), prva natuknica) – s voditeljima obrade koji su formalno izjavili da su se pridržavali tih pojednostavljenih normi koje su **izuzete** od obavješćivanja; ili
- kada nacionalno pravo države članice traži imenovanje neovisnog ***službenika za zaštitu podataka*** unutar organizacije samog voditelja obrade, koji je dužan "osigurati na neovisan način unutarnju primjenu [nacionalnih odredbi o zaštiti osobnih podataka donesenih u skladu s ovom Direktivom]" i za vođenje evidencije postupaka obrade koje provodi voditelj obrade, a sadrži iste podatke o kojima bi se inače trebalo obavijestiti nadzorno tijelo, TZP (čl. 18(2), druga natuknica).

85 Druge operacije koje mogu biti izuzete od obveze obavješćivanja bile su javne evidencije, koje su obrađivale evidencije članova i suradnika neprofitnih političkih, religijskih, filozofskih ili sindikalnih tijela pod nekim jamstvima, i ručno arhivirane zbirke (čl. 18(3) – (5)).
86 Cjelovit tekst: "za vrste obrade za koje, s obzirom na podatke koje je potrebno obraditi, nije vjerojatno da će negativno utjecati na prava i slobode osoba čiji se podaci obrađuju".

Prva iznimka temeljila se na francuskom sustavu "*normes simplifiées*"; druga na njemačkom sustavu koji zahtijeva imenovanje Službenika za zaštitu podataka unutar organizacija svih voditelja obrade iz javnog sektora i većine velikih voditelja obrade iz privatnog sektora.[87] U odnosu na oba alternativna sustava, Direktiva propisuje da voditelji obrade (ili neko drugo tijelo imenovano od strane države članice) trebaju učiniti iste informacije javno dostupnima na način kako bi i inače bile dostupne kroz evidenciju postupaka obrade (čl. 21(3)).

"Prethodna provjera":

U skladu s francuskim pristupom, Direktiva iz 1995. zahtijevala je obradu koja je predstavljala "specifične rizike za prava i slobode nositelja podataka" ("rizična obrada") koja podliježe daljnjem zahtjevu "prethodne provjere" (čl. 20). Državama članicama bilo je dopušteno odrediti koje će vrste operacija obrade podvrgnuti tom daljnjem zahtjevu (uzimajući u obzir svrhu obrade, vrste podataka i opseg predmetne obrade). Države članice također bi mogle odabrati kako i tko će izvršiti takvu provjeru, a posebno:

Direktiva iz 1995. g. zahtijevala je da obrada koja je predstavljala "**poseban rizik za prava i slobode osoba čiji se podaci obrađuju**" ("**rizična obrada**") bude podložna dodatnom zahtjevu "**prethodne provjere**" (čl. 20). Prepušteno je državama članicama da odrede **koje vrste obrade** bi one podvrgle tom dodatnom zahtjevu (uzimajući u obzir svrhu obrade, vrstu podatka i opseg dotične obrade). Države članice su također mogle odabrati **kako i tko će** izvršiti takvu provjeru, a posebno:

- treba li zahtijevati prethodnu provjeru **nakon podnošenja obavijesti** u kojoj se navodi da je prijavljena radnja bila takve vrste da je takvu provjeru zahtijevao TZP (francuski pristup, a slijedi ga većina drugih država članica); ili
- ako će se obrada regulirati zakonom ili podzakonskim aktom, TZP u tijeku pripreme instrumenta ili od strane Parlamenta, tijekom usvajanja takvog instrumenta (čl. 20(2) i (3)).

Zbog ovih različitih opcija u Direktivi, različite su države članice usvojile (odnosno, zadržale) različita uređenja u tom smislu, što je značilo da su neke operacije bile podložne obavješćivanju ili prethodnim provjerama u nekim državama članicama, ali ne i u drugima. Specifični pravni lijekovi i sankcije

Konvencija iz 1981. g. propisivala je da države članice te konvencije trebaju "*ustanoviti **odgovarajuće sankcije i pravne lijekove***" za kršenja njihovih nacionalnih zakona o zaštiti podataka, ali nije dalje obrazložila što bi bilo "odgovarajuće" u tom smislu.

Nasuprot ovoj odredbi u Konvenciji iz 1981. g., Direktiva iz 1995. je propisala da osobe čiji se podaci obrađuju imaju pravo na **pravni lijek** za svako (navodno) kršenje njihovih prava (posve odvojeno od prava ulaganja pritužbi kod nadležnog nacionalnog tijela za zaštitu podataka, što je opisano pod prethodnim podnaslovom) (čl. 22). Osim toga, svaka osoba koja je pretrpjela štetu kao rezultat bilo kojeg nezakonitog postupka obrade ili bilo kojeg djela koje je nespojivo s odredbama Direktive ima pravo od voditelja obrade zahtijevati naknadu štete (osim ako potonji može dokazati da nije bio odgovoran) (čl. 23).[88] A izvan ovih pravnih lijekova, od država članica se također tražilo da osiguraju daljnje "odgovarajuće mjere" i "sankcije", neovisno o bilo kojem individualnom zahtjevu ili pritužbi (čl. 24).

Međutim, u mnogim državama članicama stvarne kazne koje su se mogle nametnuti prema važećem nacionalnom zakonodavstvu, ili koje su nametnute u praksi, bile su relativno neznatne.[89]

---

87 Koji se nazivaju *behördliche-* i *betriebliche Datenschutzbeauftragten*, te ih se ne smije pomiješati s državnim i saveznim tijelima za zaštitu podataka, *Landes-* i *Bundesdatenschutzbeauftragten*.

88 Ujedinjeno Kraljevstvo je na početku pokušalo ograničiti ovo samo na materijalnu štetu, ali je na kraju zauzet stav da Direktiva traži da osobe također moraju biti u mogućnosti dobiti naknadu i za nematerijalnu štetu (nanošenje boli).

89 Potreba za strožim kaznama postala je očigledna tek pojavom interneta, uvelike kontroliranog od strane osoba izvan EU/EGP-a za koje je postojala manja vjerojatnost da će poštivati pravila o zaštiti podataka EU-a, a i ovo samo na nagovor TZP-ova iz EU-a. Ovo se vidi u mnogo snažnijem definiranju odredaba u GDPR-u, prema kojima TZP-ovi mogu nametnuti upravne novčane kazne u iznosu do 10.000.000 € ili 2 % godišnjeg prometa odgovornog počinitelja, ili u doista posebno teškim slučajevima u iznosu do 20.000.000 € ili 4 % godišnjeg prometa (čl. 83 GDPR-a).

Radna skupina iz članka 29. i Odbor iz članka 31.

Na kraju, Direktiva o zaštiti podataka iz 1995. g. ustanovila je dv TZP-ovi U, nazvana po člancima temeljem kojih su osnovana:

- tzv. "**Radna skupina iz čl. 29"**, neovisna skupina sastavljena od predstavnika nadzornih tijela država članica, kao i Europskog nadzornika za zaštitu podataka (ENZP), te predstavnika Europske komisije (zaduženog za obavljanje poslova tajništva skupine, bez prava glasa), kojoj je dana zadaća da doprinosi usklađenijoj primjeni Direktive, prvenstveno usvajajući preporuke i mišljenja (na vlastitu inicijativu) te davanjem mišljenja na bilo koji nacrt kodeksa ponašanja na razini EU, te je Europska komisija dužna savjetovati se sa skupinom o bilo kojem prijedlogu vezanom za "*prava i slobode fizičkih osoba u vezi obrade osobnih podataka*" (tj., zaštitu podataka) i o svim prijedlozima odluka o odgovarajućoj razini zaštite u trećoj državi;[90] i
- tzv. "**Odbor iz čl. 31**", sastavljen od predstavnika vlada država članica, uz predsjedavanje predstavnika Komisije, kojem se podnese svi prijedlozi mjera koje je potrebno poduzeti po Direktivi da bi odbor donio svoje mišljenje; ako je Odbor donio negativno mišljenje, mjera se mora uputiti Vijeću, gdje može biti donesena drugačija odluka kvalificiranom većinom.[91]

Radna skupina iz čl. 29 (RS29) izradila je **brojne radne dokumente i mišljenja** o iznimno širokom rasponu pitanja koja se odnose na primjenu Direktive o zaštiti podataka iz 1995. g. i Direktive o e-privatnosti iz 2002. g. (opisano pod točkom 1.3.3, u nastavku teksta).[92] Ti dokumenti, a posebno formalna mišljenja, premda nisu pravno obvezujuća, i dalje imaju visok autoritet u smislu direktiva. Pomogla su u osiguravanju da se direktive doista cjelovito i dosljedno primjenjuju, na "visokoj razini", te moraju u nekoj mjeri umanjiti probleme koji se javljaju zbog odstupanja među zakonima u državama članicama.

Bilješka: Nasljednik RS29-a, Europski odbor za zaštitu podataka (*the European Data Protection Board*, EOZP), nastavlja dalje na radu RS29-a: na prvi dan svog postojanja, 25. svibnja 2018. g., potvrdio je čitav raspon mišljenja RS29, koja su donesena u očekivanju GDPR-a.[93] Njezino tajništvo osigurano je od strane ENZP-a.

1.3.2 Direktiva o zaštiti telekomunikacijskih podataka iz 1997., Direktiva o e-privatnosti iz 2002. i izmjene i dopune Direktive o e-privatnosti iz 2009. godine

OPĆENITO

Direktiva o zaštiti podataka u telekomunikacijama, predložena istodobno kada i Direktiva o zaštiti podataka iz 1995. g., usvojena je 15. rujna 1997. g.[94] Njezin odnos s Direktivom o zaštiti podataka iz 1995. g. razjašnjen je u čl. 1(2), koji navodi da odredbe direktive trebaju "*specificirati i dopuniti*" glavnu Direktivu. Posebice, specifične definicije vezane za zaštitu podataka Direktive iz 1995. g., kao i sva ostala načela i pravila iz direktive, primijenjeni također i na voditelje obrade i na operacije obrade na koje se primjenjuje Direktiva o zaštiti podataka u telekomunikacijama, osim gdje je potonja iznijela posebnija ili različita pravila.

90 Za pojedinosti, vidjeti članak 30.
91 Za pojedinosti, pogledati Članak 31.
92 Svi dokumenti Radne skupine iz Čl.29 usvojeni između 1997. i studenog 2016.g. možete pronaći na poveznici: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm
Ažurirane verzije i dokumenti usvojeni nakon studenog 2016.g. pa sve do ukidanja WP29 na dan 25. svibnja 2018.g., mogu se pronaći ovdje: http://ec.europa.eu/newsroom/article29/news-overview.cfm
93 Vidi fusnotu 215, dolje.
94 Puni naziv: Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24, 30.01.1998, pp. 1 – 8, dostupno na (ENG): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN Direktiva o zaštiti podataka u telekomunikacijama uvelike se oslanjala na rad obavljen u okviru Vijeća Europe vezano za preporuku o istom pitanju, što je dovelo do usvajanja Preporuke - Recommendation No. R (95) 4 of the Committee of Ministers of the Council of Europe to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with particular reference to Telephone Services, usvojene 7. veljače 1995.g., dostupno na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805010 8e i na rad Međunarodne radne grupe za zaštitu podataka u telekomunikacijama (the International Working Group on Data Protection in Telecommunications, tzv. "Berlin Group"), osnovanu 1983.g., pogledati: https://www.dataprotectionauthority.be/berlin-group

Drugim riječima, Direktiva o zaštiti podataka u telekomunikacijama bila je *lex specialis* u odnosu na Direktivu o zaštiti podataka iz 1995. g., koja je bila *lex generalis*.

Provedba ove direktive bila je odgođena, djelomično zato što je 1999. godine Komisija provela opći pregled regulatornog okvira za elektroničke komunikacije, u svjetlu razvoja novih tehnologija i poslovnih praksi. Jedan rezultat ove revizije bio je prijedlog 2000. godine za zamjenu Direktive o zaštiti podataka u telekomunikacijama novom direktivom koja se odnosi na zaštitu podataka u sektoru elektroničkih komunikacija.[95] U srpnju 2002. godine, to je dovelo do usvajanja Direktive o privatnosti i elektroničkim komunikacijama, Direktive 2002/58/EZ, općenito nazvane "**Direktiva o e-privatnosti**".[96] Ona je također naglasila svoju pomoćnu i komplementarnu prirodu u odnosu na glavnu Direktivu o zaštiti podataka iz 1995. g., korištenjem istih termina kao i njena prethodnica (vidjeti čl. 1(2)).

Direktiva iz 2009, izmijenjena je 2002. posebnom direktivom, Direktivom 2009/136/EZ[97], koja se često naziva "Zakonom o kolačićima", jer regulira kolačiće (iako je također regulirala daljnje dodatne poslove i aktivnosti obrade podataka). U tekstu koji slijedi opisat ćemo pravila koja su sadržana u Direktivi iz 2002. kako je izmijenjena i dopunjena Direktivom iz 2009. godine. Radi kratkoće, povremeno ćemo upućivati na Direktivu o zaštiti podataka iz 1995. kao "glavnu direktivu", a na Direktivu o e-privatnosti (kako je izmijenjena) kao svoju "dopunsku" direktivu.

U vrijeme pisanja (prosinac 2018.), Direktiva o e-privatnosti je još uvijek na snazi, iako je njen "majčinski" instrument, Glavna direktiva o zaštiti podataka iz 1995., zamijenjen Općom uredbom o zaštiti podataka. Nasljednik Direktive o e-privatnosti, koja bi također trebala biti propis (a ne direktiva), trenutno je u procesu usvajanja (vidi odjeljak 1.4.2. u nastavku). Međutim, Direktiva o e-privatnosti će ostati na snazi - zbog čega je još uvijek posvećena puna pažnja ovom prvom izdanju priručnika i zašto, dok se ne usvoji predložena nova Uredba o e-privatnosti, u nastavku ćemo opisati još uvijek primjenjivu Direktivu o e-privatnosti.

Cilj, svrha i područje primjene Direktive o e-privatnosti iz 2002., izmijenjena 2009.

Dok se glavna Direktiva o zaštiti podataka iz 1995. g. široko primjenjivala na svaku obradu osobnih podataka od strane tijela iz javnog ili privatnog sektora, aktivnog u "prvom stupu" Europske zajednice, za to vrijeme je Direktiva o e-privatnosti, kao pomoćni instrument, imala mnogo uže područje primjene. Primjenjuje se na:

> obradu osobnih podataka u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u Zajednici, uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i uređaje za identifikaciju (članak 3, naglasak dodan; riječi kurzivom dodane su izmjenom iz 2009.)[98]

Pojam "elektroničke komunikacijske usluge" je točno i strogo definiran u članku 2. točki (c) revidirane Okvirne direktive,99 kako slijedi:

---

95 Prijedlog Direktive Europskog parlamenta i Vijeća vezano za obradu osobnih podataka i zaštitu privatnosti u sektoru elektroničkih komunikacija (*the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Brussels, 12.07.2000, COM(2000) 385 final.

96 Puni naziv: Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (*Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, SL L201, 31.07.2002, pp. 37 – 47, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32002L0058&from=HR

97 Puni naziv: Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredba (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača, SL L337, 18.12.2009., str., dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136

98 Iznimka za analogne razmjene, sadržana u izvornoj (2002.) verziji Direktive o e-privatnosti, uklonjena je izmjenama iz 2009. godine.

99 Puni naziv: Direktiva 2002/21/EZ Europskog Parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva) SL L 108, 24.4.2002., Str. 33-50, dostupno na: https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:32002L0021

"elektronička komunikacijska usluga" znači usluga koja se uobičajeno pruža uz naknadu i sastoji se u cijelosti, ili većim dijelom, od prijenosa signala u elektroničkim komunikacijskim mrežama, uključujući telekomunikacijske usluge i usluge prijenosa u radiodifuzijskim mrežama, ali isključujući usluge pružanja sadržaja i obavljanja uredničkog nadzora nad sadržajem koji se prenosi korištenjem elektroničkih komunikacijskih mreža i usluga; **ona ne obuhvaća usluge informacijskog društva, u skladu s definicijom iz članka 1. Direktive 98/34/EZ,[100] koje se ne sastoje, u cijelosti ili većim dijelom, od prijenosa signala u elektroničkim komunikacijskim mrežama** (naglasak dodan);

Jednostavan zaključak koji proizlazi iz ove odredbe u članku 3. i definicije u tim instrumentima izradio je RS29 2011. g. u svom Mišljenju o uslugama geolokacije na pametnim mobilnim uređajima:[101] Direktiva o e-privatnosti primjenjuje se na pružatelje usluga e-komunikacije kao što su telekomunikacijski operatori te internet poslužitelji, ali ne pružatelji usluga informacijskog društva.[102]

(Kao što je dalje objašnjeno u odjeljku 1.4.2., Komisija predlaže uklanjanje ovog ograničenja prema predloženoj Uredbi o e-privatnosti, ali dok se to ne učini, ona ostaje na snazi.)

U tom ograničenom opsegu, Direktiva o e-privatnosti ima iste ciljeve kao i glavna Direktiva: istodobno osigurati **visoku razinu zaštite** osobnih podataka (ali ovdje posebno za taj sektor) i omogućiti **slobodan protok osobnih podataka** unutar Zajednice (unutar tog sektora) (usp. članak 1, stavak 1). To je imalo velik utjecaj na brzo rastuće, sve važnije područje e-komunikacija, osiguravajući višu razinu zaštite podataka na tom području unutar EU nego bilo gdje drugdje u svijetu.

Međutim, unatoč naizgled jasnom jeziku članka 3., pitanje preciznog područja primjene Direktive o e-privatnosti nije potpuno jasno, jer se neke njegove odredbe primjenjuju - ili se čitaju kao da se primjenjuju - šire; i zato što Direktiva o e-privatnosti ne sadrži izričitu odredbu u odnosu na mjerodavno pravo. Ne utječući na uspjeh Direktive o e-privatnosti, te nejasnoće treba ukratko spomenuti.

Dvosmislenost i nedostatak usklađenosti u pogledu opsega

Prvenstveno, postoje dvosmislena tumačenja opsega materije Direktive o e-privatnosti.

Kao što je Komisija navela u svom prijedlogu Uredbe o e-privatnosti:[103]

Potrošači i poduzeća sve se više oslanjaju na nove internetske usluge koje omogućuju interosobne komunikacije, kao što su Voice over IP, *instant messaging* i web usluge e-pošte, umjesto tradicionalnih komunikacijskih usluga. **Te komunikacijske usluge ("OTT") *u pravilu* ne podliježu sadašnjem okviru Unije za elektroničke komunikacije, uključujući Direktivu o e-privatnosti.**

Studija iz 2013., provedena temeljem zahtjeva Komisije (The SMART Study) utvrdila je da

100 Puni naziv: Direktiva 98/34/EZ Europskog Parlamenta i Vijeća od 22. lipnja 1998. o utvrđivanju postupka osiguravanja informacija u području tehničkih normi i propisa, OJ L 204, 21.07.1998., str. 37-48, dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31998L0034

101 Radna skupina iz članka 29., Mišljenje 13/2011 o uslugama geolokacije na pametnim mobilnim uređajima (WP185, usvojeno 16. svibnja 2011.), dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

102 RS29 Mišljenje 13/2011 o uslugama geolokacije na pametnim mobilnim uređajima (prethodna bilješka), odjeljak 4.2.1, Primjenjivost revidirane direktive o e-privatnosti (str. 8-9).
Kao što je još preciznije navedeno u radnom dokumentu Komisije (napomena 99, iznad):
"*Da bude obuhvaćena Direktivom:*
(1) *usluga treba biti usluga elektroničkih komunikacija,*
(2) *usluga treba biti ponuđena u elektroničkoj komunikacijskoj mreži,*
(3) *spomenuta usluga i mreža trebaju biti javno dostupne, i*
(4) *mreža ili usluga trebaju biti osigurane u Zajednici.*" (str.20)
Kao što je dalje objašnjeno u odjeljku 1.4.2., Komisija predlaže uklanjanje tog ograničenja u okviru predložene Uredbe o e-privatnosti, ali dok to ne bude učinjeno, ona ostaje na snazi.

103 Prijedlog Uredbe o e-privatnosti (bilješka 175, ispod), odjeljak 1.1, str. 1, dodani su naglasci.

nacionalne odredbe o temama kao što su kolačići, podaci o prometu i lokaciji ili neželjene komunikacije, usvojene u skladu s Direktivom o e-privatnosti, često imaju različit opseg primjene od onog definiranog člankom 3. Direktive o e-privatnosti, koja je ograničena samo na pružateljima javno dostupnih usluga elektroničkih komunikacija (tj. tradicionalnih telekomunikacijskih tvrtki). [Studija je utvrdila] da je ograničenje područja primjene Direktive samo na pružatelje elektroničkih komunikacijskih usluga dvosmisleno i da može dovesti do nejednakog tretmana ako pružatelji usluga informacijskog društva koji koriste internet za pružanje komunikacijskih usluga uglavnom nisu obuhvaćeni njegovim područjem primjene.

Također, nije u potpunosti jasna pozicija *u odnosu na mjerodavno nacionalno pravo:*

Dok se Direktiva o e-privatnosti ne zamijeni predloženom Uredbom o e-privatnosti (koja možda neće biti neko vrijeme), gore navedene nejasnoće i nejasnoće će ostati, a djelotvornost Direktive o e-privatnosti i dalje će biti time ometena.

ODNOS IZMEĐU DIREKTIVE O E-PRIVATNOSTI I GDPR-A

Direktiva o e-privatnosti bila je *lex specialis* u odnosu na *lex generalis* Direktivu iz 1995, slijedom čega je također *lex specialis* u odnosu na nasljednika, odnosno GDPR. U **pogledu pitanja koja su posebno uređena Direktivom o e-privatnosti**, Direktiva o e-privatnosti primjenjuje se umjesto odredbi GDPR-a.

Stoga pravna osnova GDPR-a nije primjenjiva kada Direktiva o e-privatnosti propisuje specifičnija pravila za obradu osobnih podataka. Primjerice, primjenjuje se Direktiva o e-privatnosti iz članka 6. koja određuje poseban popis pravnih osnova u vezi s obradom podataka o prometu, uključujući podatke o prometu koji čine osobne podatke, a time članak 6. GDPR-a nije primjenjiv. Međutim, u svim ostalim slučajevima koji se odnose na obradu osobnih podataka, primjenjuje se GDPR.

Isto vrijedi i za **subjekte koji jesu, ili nisu, "posebno uređeni Direktivom o e-privatnosti"**. S obzirom na mišljenje RS29 da se Direktiva o e-privatnosti bitno primjenjuje samo na pružatelje usluga e-komunikacije, to znači da na sličan način (osim u odnosu na posebna pravila u članku 5. stavku 3. i članku 13. koji se primjenjuju šire), obrada svih podataka, uključujući podatke koji su specifičnije uređeni Direktivom o e-privatnosti (kao što su podaci o prometu) od strane subjekata koji nisu pružatelji usluga e-komunikacije, podliježe direktivi GDPR, a ne Direktivi o e-privatnosti, unatoč posebnim odredbama u Direktivi o e-privatnosti koje se odnose na takve podatke.

Drugim riječima:

- pružatelji usluga e-komunikacije moraju se pridržavati Direktive o e-privatnosti u odnosu na sva pitanja koja su specifičnije uređena u toj direktivi, kao i GDPR u odnosu na sva ostala pitanja; i
- subjekti koji nisu pružatelji usluga e-komunikacije moraju se pridržavati odredbi iz članka 5. stavka 3. Direktive o e-privatnosti u vezi s pristupom informacijama na uređajima i člankom 13. te direktive koje se odnose na neželjena priopćenja i GDPR u odnosu na sva druga pitanja (tj. ne podliježu nijednoj odredbi u Direktivi o e-privatnosti, osim ove dvije odredbe).

Posebni problemi koji se javljaju na gore navedena pitanja zabilježena su tamo gdje su relevantna u drugim pododjeljcima ovog odjeljka.

Ključne značajke Direktive o e-privatnosti104

Definicije

S obzirom da je Direktiva o e-privatnosti izrijekom zamišljena kao *lex specialis* u odnosu na *lex generalis*, tj. Direktivu o zaštiti podataka iz 1995. g., **definicije koje se odnose na zaštitu podataka** iz Direktive o zaštiti podataka iz 1995. g. također se primjenjuju u odnosu na

Direktivu o e-privatnosti, kao što je izričito navedeno člankom 2., prva rečenica Direktive o e-privatnosti. Međutim, sada kada je Direktiva o zaštiti podataka iz 1995. zamijenjena GDPR-om, sva upućivanja na definicije u toj direktivi trebala bi se tumačiti kao upućivanja na odgovarajuće (ali u određenim aspektima ažurirane i ojačane) definicije u Uredbi. To je navedeno u nastavku, posebno pod posebnim naslovom "Privola".[105]

Osim toga, **definicije tehničkih pojmova vezanih uz e-komunikacije** u Okvirnoj direktivi o elektroničkim komunikacijskim mrežama i uslugama,[106] koje su rezultat gore spomenutog pregleda, pod naslovom "*Općenito*" ***- usluga elektroničkih komunikacija;***[107] ***javno dostupna elektronička komunikacijska usluga; javna komunikacijska mreža; itd.*** - također se primjenjuju na relevantne tehničke pojmove koji se koriste u Direktivi o e-privatnosti. To uključuje izraz "pretplatnik" (na uslugu e-komunikacije).

Osim toga, u članku 2., Direktiva o e-privatnosti dodaje **nekoliko (novih) definicija**, kao što su ***"korisnik", "podaci o prometu", "podaci o lokaciji", "usluge s dodanom vrijednošću"*** i ***"povreda osobnih podataka"*** (vidi članak za detalje).

Privola

Najvažnija promjena definicije temeljnih koncepata u GDPR-u u usporedbi s onima iz Direktive o zaštiti podataka iz 1995. g. odnosi se na definiciju "privole" kao pravne osnove za obradu osobnih podataka.

> Konkretno, članak 2 (f) Direktive o e-privatnosti propisuje da "pristanak" korisnika ili pretplatnika, kako se to navodi u Direktivi, odgovara suglasnosti nositelja podataka u Direktivi o zaštiti podataka. Budući da se sva upućivanja na Direktivu o zaštiti podataka sada moraju tumačiti kao pozivanje na GDPR, suglasnost u skladu s Direktivom o e-privatnosti sada mora biti shvaćen na isti način kao i pristanak u okviru GDPR-a, koji je definiran kao "svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim želi da on ili ona, izjavom ili jasnom pozitivnom odlukom, označava pristanak na obrada osobnih podataka koji se odnose na njega ili nju (čl. 4(11) GDPR-a)".
>
> GDPR također pojašnjava koji sve uvjeti moraju biti ispunjeni kako bi se određeni pristanak/suglasnost smatrali valjanim te određuje, između ostalog, što znači da se pristanak slobodno daje, a što mora predstavljati jasnu potvrdnu radnju.[108] Europski odbor za zaštitu podataka (EOZP) je također izdao smjernice vezane za pristanak/privolu.[109]
>
> > Pojašnjenja u GDPR-u i u ovom priručniku posebno su relevantna u odnosu na nekoliko ključnih odredbi Direktive o e-privatnosti vezano za privolu koju voditelj obrade mora pribaviti od korisnika ili pretplatnika za obradu njegovih osobnih podataka. To uključuje:
> >
> > - članak 5.3. za pohranjivanje ili prikupljanje informacija koje odašilje terminalna oprema;
> > - članke 6. i 9. za ponovno korištenje podataka o prometu i lokaciji za usluge s dodanom vrijed-

104 Mnogi zahtjevi iz Direktive o e-privatnosti, koji su ovdje spomenuti, već su sadržani u Direktivi o zaštiti podataka o telekomunikacijama iz 1997. godine i samo su preneseni na Direktivu o e-privatnosti, ali to se dalje ne navodi u svakom pojedinom slučaju.
105 GDPR također pomalo dodatno pojašnjava pojam "osobnih podataka", jasno stavljajući do znanja da osoba može biti "prepoznatljiva" putem "mrežnog identifikatora" (čl. 4 (1) GDPR, čl. Direktive o zaštiti podataka iz 1995.godine). I to bi se sada trebalo uzeti u obzir i u primjeni Direktive o e-privatnosti.
106 Bilješka 97, iznad.
107 Ovaj je termin razmotren gore, pod naslovom "Cilj, svrha i djelokrug Direktive o e-privatnosti".
108 Vidjeti čl. 7 i 8 GDPR-a te povezane uvodne izjave 32-33 i 42-43.
109 Smjernica EOZP-a o pristanku/privoli sukladno Regulativi 2016/679 (RS259rev.01). Predmetne smjernice usvojene su čl. 29. Radne skupine (RS29) 28. studenog 2017. te izmijenjene 10. travnja 2018. Također, smjernice je odobrilo tijelo koje je nasljedilo Radnu skupinu (RS29), Europski odbor za zaštitu podataka (EOZP) te su nadopuna prethodnom mišljenju radne skupine koje se odnosi na definiciju pristanka/privole (WP187, mišljenje, 15/2011).

nošću u svrhu marketinga elektroničkih komunikacijskih usluga;

- članak 12. za imenike pretplatnika; i
- članak 13. za neželjene komunikacije.

U odnosu na navedeno, privola, da bi bila valjana, sada mora biti "privola iz GDPR-a" te su države članice dužne uskladiti nacionalne zakone koji prenose Direktivu o e-privatnosti i nacionalne provedbene prakse s GDPR-om.

Gore spomenuta pitanja su u nastavku razmatrana pod odgovarajućim naslovima.

Sigurnost

Članak 4(1) učinkovito ponavlja zahtjev sigurnosti podataka iz Direktive o zaštiti podataka iz 1995. g., propisujući da pružatelji (davatelji) elektroničkih komunikacijskih usluga moraju poduzeti "***odgovarajuće tehničke i organizacijske mjere kako bi zaštiti[li] sigurnost svojih usluga***", dodajući da "*ako je potrebno*", ovo mora biti učinjeno "*zajedno s davateljem [dotične] javne komunikacijske mreže*". Također dodaje, kao i glavna Direktiva, da razina sigurnosti mora osigurati "***razinu sigurnosti koja odgovara prikazanim opasnostima***", uzimajući u obzir najnovija dostignuća i trošak provedbe mjera. Članak 4 (1a), uveden Direktivom iz 2009., dodaje da:

Ne dovodeći u pitanje Direktivu 95/46/EZ, mjere iz stavka 1. moraju najmanje:

- osigurati da osobnim podacima mogu pristupiti samo ovlaštene osobe u zakonski dopuštene svrhe,
- zaštititi osobne podatke pohranjene ili prenesene od slučajnog ili nezakonitog uništenja, slučajnog gubitka ili promjene, te neovlaštenog ili nezakonitog pohranjivanja, obrade, pristupa ili otkrivanja, i,
- osigurati provedbu sigurnosne politike u pogledu obrade osobnih podataka.

prethodnom čl. 29 mišljenja radne skupine koje se odnosi na definiciju pristanka/privole (RS187, mišljenje, 15/2011).

I Direktiva o e-privatnosti (u čl. 4) i GDPR (u čl. 32 - 34) predviđaju obvezu osiguranja sigurnosti, kao i obvezu prijavljivanja povreda osobnih podataka nadležnom nacionalnom tijelu i nadzornom tijelu [tj. tijelu za zaštitu podataka].[110] Te će obveze paralelno postojati u okviru dva različita zakonodavstva, u skladu s njihovim opsegom primjene. U skladu s člankom 95. GDPR-a, GDPR ne nameće dodatne obveze fizičkim ili pravnim osobama u vezi s pitanjima za koja su predmet posebnih obveza utvrđenih u Direktivi o e-privatnosti. Međutim, kao *lex specialis* za GDPR, e-privatnost ne bi trebala [također] dovesti do niže razine zaštite od zaštite koju pruža GDPR. Članak 4. stavak 1. također propisuje da:

> Nadležna nacionalna tijela moći će provjeravati mjere koje provode pružatelji javno dostupnih elektroničkih komunikacijskih usluga te izdavati preporuke o najboljim praksama u pogledu razine sigurnosti koju bi te mjere trebale postići.

Napominjemo da ta "nadležna tijela" ne moraju biti nacionalna tijela za zaštitu podataka. Vidi pod naslovom "Nadzor i provedba", ispod.

Obavijest o riziku

Članak 4 (2) Direktive o e-privatnosti propisuje da:

U slučaju **posebne opasnosti od narušavanja sigurnosti mreže**, pružatelj javno dostupne elektroničke komunikacijske usluge mora obavijestiti pretplatnike o takvoj opasnosti te, ako opasnost leži izvan opsega

110 Što se tiče različitih tijela uključenih u provedbu Direktive o e-privatnosti, pogledajte sljedeći citat u ovom pododjeljku i komentar na njega, te raspravu pod posljednjim naslovom u ovom odjeljku.

mjera koje treba poduzeti davatelj usluge, o **mogućim sredstvima za otklanjanje opasnosti**, uključujući i naznaku vjerojatnih **troškova** koji će se s tim u vezi pojaviti. (dodani naglasci)

Ovaj zahtjev za "obavješćivanje o riziku/opasnosti" (koji je već bio uključen u izvorni tekst iz 2002.) treba razlikovati od zahtjevnijih zahtjeva za "obavješćivanje o povredi osobnih podataka", koji se razmatraju u sl

jedećem poglavlju - koji su dodani samo u izmjenama iz 2009. godine, a koji se primjenjuju samo nakon što je došlo do kršenja, dok članak 4. stavak 2. zahtijeva obavijest o svakom riziku do čijeg kršenja može doći.

Obavijest o kršenju podataka

Direktiva o e-privatnosti (izmijenjena i dopunjena 2009. godine) propisuje da, osim gore navedenog zahtjeva o obavijesti o riziku, pružatelji usluga e-komunikacije moraju **obavijestiti "nadležno nacionalno tijelo"** o - pročitati *svaku stvarnu* - povredi osobnih podataka *"bez nepotrebnog odgađanja"* (čl. 4 (3), prva podtočka - napominjemo da ovo tijelo opet ne mora biti TZP).

Ako (ali samo ako) "*povreda osobnih podataka* ***može negativno utjecati na osobne podatke ili privatnost pretplatnika ili pojedinca***", tada pružatelj također mora "***obavijestiti pretplatnika ili pojedinca***" o kršenju "bez nepotrebnog odlaganja" (čl. 4 (3), druga podtočka). Međutim, takva obavijest pretplatniku ili pojedincu nije potrebna:

> ako je pružatelj usluga nadležnom tijelu dokazao da je proveo odgovarajuće mjere tehnološke zaštite, te da su te mjere primijenjene na podatke o kojima je riječ o kršenju sigurnosti. Takve tehnološke mjere zaštite učinit će podatke nerazumljivima bilo kojoj osobi koja nije ovlaštena pristupiti podacima (čl. 4 (3), treća podtočka).

Drugim riječima, pretplatnici i ostali zahvaćeni pojedinci (posebno naravno, subjekti podataka, ali i pravni subjekti koji su pretplatnici) ne moraju biti obaviješteni o kršenju podataka koji uključuje njihove podatke ako pružatelj može dokazati "nadležnom tijelu" da podaci koji su bili ugroženi (osobito, bilo koji podaci koji su možda nepropisno objavljeni ili dostupni trećim stranama) bili su potpuno "nerazumljivi" bilo kojoj osobi ili osobama koje su možda dobile pristup kao rezultat kršenja, odgovarajućom tehnološkom mjere zaštite (kako je pojašnjeno u članku 4. Uredbe Komisije 611/2013).[111]

Nasuprot tome, "nadležno tijelo" može "zahtijevati" od pružatelja usluga da obavijesti povredu podataka relevantnim pretplatnicima i drugim zahvaćenim osobama kada pružatelj nije to učinio - tj. zato što se tijelo ne slaže s procjenom pružatelja da kršenje podataka nije "*moglo negativno utjecati*" na osobne podatke ili privatnost tih pretplatnika ili pojedinaca, ili zato što tijelo ne vjeruje da su podaci koji su procurili doista potpuno "nerazumljivi" za neovlaštene primatelje (npr. jer je ključ za dešifriranje bio ili je također mogao procuriti, ili zato što metoda šifriranja nije bila dovoljno čvrsta)[112] (čl. 4, st. 3, četvrta podtočka).

---

111 Puni naziv: Uredba Komisije (EU) br. 611/2013 od 24. lipnja 2013. o mjerama koje se primjenjuju na obavješćivanje o povredama osobnih podataka u skladu s Direktivom 2002/58/EZ Europskog parlamenta i Vijeća o privatnosti i elektroničkim komunikacijama, SL 173 od 26.06.2013., str. 2-8, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611

Uredba Komisije usvojena je na temelju članka 4. stavka 5. Direktive o e-privatnosti, koja ga je ovlastila da usvoji "*tehničke provedbene mjere koje se odnose na okolnosti, format i postupke koji se primjenjuju na zahtjeve obavješćivanja i obavješćivanja iz ovog članka*" (čl. 4, st. 5), nakon savjetovanja s Europskom agencijom za sigurnost mreža i informacija (ENISA), RS29 i ENZP-om, te uključivanjem svih (drugih) relevantnih dionika.

112 Na primjer, slabi algoritmi kao što su MD5 ili SHA1 smatraju se zastarjelima, a za podatke koji se šifriraju preko njih više se ne može smatrati da su učinjeni "nerazumljivim" (čitaj: un-decryptable). Vidjeti:

https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
Može se zamisliti i slučaj u kojem se krše podaci o e-komunikacijama, u kojima je sadržaj komunikacija potpuno šifriran pomoću jakih algoritama kao što je SHA-256, ali metapodaci nisu. Imajte na umu da (kao što je istaknuto na gore navedenoj web-lokaciji) "klasifikacija" jakog "kriptografskog algoritma može se mijenjati tijekom vremena".

Konačna, peta podtočka članka 4. stavka 3. propisuje da:

> Obavijest pretplatniku ili pojedincu mora barem opisati prirodu povrede osobnih podataka i kontaktne točke gdje se može dobiti više informacija te će preporučiti mjere za ublažavanje mogućih štetnih učinaka povrede osobnih podataka. Obavijest nadležnom nacionalnom tijelu, osim toga, opisuje posljedice i mjere koje je pružatelj pružio ili poduzimao za rješavanje povrede osobnih podataka.

Direktiva o e-privatnosti kako je izmijenjena i dopunjena Direktivom iz 2009. također predviđa važne formalne zahtjeve za podupiranje gore navedenih novih odredbi. Tako: [Nadležna nacionalna tijela] također će moći **provjeravati** jesu li pružatelji usluga ispunili svoje obveze obavješćivanja u skladu s ovim stavkom, te će izreći odgovarajuće **sankcije** u slučaju da to ne učine (članak 4 (4), prva podtočka, druga rečenica).

Učinkovitost tih ovlasti revizije (inspekcije) i sankcioniranja podupire se daljnjim zahtjevom navedenim u drugom podstavku članka 4 (4):

> Pružatelji će održavati popis povreda osobnih podataka koje obuhvaćaju činjenice vezane za kršenje, njegove učinke i poduzete korektivne mjere koje će biti dovoljne da nadležnim nacionalnim tijelima omoguće provjeru usklađenosti s odredbama stavka 3. Popis će sadržavati samo podatke u tu svrhu. (naglasak dodan)

Izmijenjena Direktiva o e-privatnosti predviđa izdavanje "**smjernica**" i "**uputa**" od strane "nadležnih nacionalnih tijela" o "*okolnostima u kojima su pružatelji usluga dužni prijaviti povrede osobnih podataka, oblik takve obavijesti i način na koji obavijest se podnosi*" (članak 4, stavak 4, prva podtočka, prva rečenica).

Navedeni zahtjevi obavješćivanja o kršenju obveza iz Direktive o e-privatnosti, koji su ograničeni područjem primjene te direktive, ukazuju na općenitije zahtjeve obavješćivanja o kršenju podataka koji su sada uključeni u Opću uredbu o zaštiti podataka, primjenjivu na bilo koju operaciju obrade osobnih podataka, navedenu u Drugom dijelu, odjeljak 2.1. Zahtjevi obavješćivanja o kršenju obveza u Direktivi o e-privatnosti mogu se smatrati "suvišnim".[113]

POSEBNI ZAHTJEVI ZA OBRADU U POSEBNE SVRHE:

Umjesto ponavljanja općih načela zaštite podataka i popisa pravnih osnova za obradu koja su navedena u glavnoj Direktivi o zaštiti podataka iz 1995., Direktiva o e-privatnosti propisuje opći zahtjev povjerljivosti komunikacija, niz posebnih zahtjeva i uvjeta za određene specifične podatke ili postupke obrade. U njima, Direktiva o e-privatnosti nastoji primijeniti načela i prava iz Direktive o zaštiti podataka iz 1995. na ta specifična pitanja, s ciljem usklađivanja primjene tih načela i prava u državama članicama, o čemu se raspravlja u raznim poglavljima ispod.

Prvo, međutim, važno je podsjetiti da, u mjeri u kojoj Direktiva o e-privatnosti predviđa posebne pravne osnove za obradu za posebne svrhe (kako je navedeno u toj direktivi), općenitiji pravni temelj za obradu u različite svrhe postavljen u člancima 5 i 6 GDPR-a se ne primjenjuju.[114]

Prema tome, kada Direktiva o e-privatnosti zahtijeva pristanak - kao što je to slučaj s pristupom informacijama na uređajima (čl. 5. (3)), ili slanjem neželjenih marketinških poruka (čl. 13) - ili određuje niz posebnih pravnih osnove i svrhe obrade - kao i u vezi s obradom podataka o prometu (čl. 6) - bilo koji subjekt koji podliježe tim pravilima - koji je u odnosu na članke 5. (3) i 13. bilo koji entitet, u odnosu na članak 6. pružatelji usluga e-komunikacije - ne mogu se oslanjati na bilo koji drugi temelj ili načelo koji su navedeni u GDPR-u. Osobito

113 Europska komisija, REFIT analiza usklađenosti Direktive o e-privatnosti s GDPR-om (grafikon - komentar na članak 4.3; 4.4; 4.5. Obavijest o kršenju osobnih podataka).
114 Vidi pododlomak "Odnos između Direktive o e-privatnosti i GDPR-a", iznad.

se ne mogu osloniti na "usklađene svrhe" za obradu, navedene u članku 5. stavku 1. točki (b) GDPR-a.

Povjerljivost komunikacije:

Članak 5 (1) Direktive o e-privatnosti naglašava temeljnu važnost povjerljivosti komunikacija - sadržanih u mnogim ustavima, barem što se tiče poštanskih i telefonskih poziva (iako se sada često izričito ili putem tumačenja proširuju na sve oblike komunikacije)[115] - propisivanjem da države članice moraju:

> osigurati **povjerljivost komunikacija i povezanih podataka o prometu** putem javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga, putem nacionalnog zakonodavstva. Osobito će ***zabraniti slušanje, prisluškivanje, pohranjivanje ili druge vrste presretanja ili nadzora komunikacija i srodnih podataka o prometu od strane osoba koje nisu korisnici***, bez **pristanka** zainteresiranih korisnika, osim kad je to zakonski dopušteno… (dodani naglasci)

Budući da riječi "*slušanje, prisluškivanje [itd.]… od strane osoba koje nisu korisnici*" jasno pokazuju, ova se odredba ne odnosi samo na pružatelje usluga e-komunikacije. Umjesto toga (u skladu s dolje navedenim iznimkama), države članice moraju, prema svojim nacionalnim zakonima, zabraniti takvo miješanje u pravo na povjerljivost komunikacija od strane **bilo koga**, uključujući državne agencije i privatne subjekte kao što su kompanije.

Članak 5. stavak 1. dopušta kao iznimku "*tehničko skladištenje koje je nužno za prijenos komunikacije, ne dovodeći u pitanje načelo povjerljivosti*". U članku 5. stavku 2. postoji daljnja iznimka u odnosu na bilježenje komunikacija i podataka o prometu radi pružanja dokaza o komercijalnoj transakciji ili poslovnoj komunikaciji. Takozvana Direktiva o zadržavanju podataka, ukratko objašnjena u točki 1.3.4, u nastavku, predviđala je daljnju, sveobuhvatnu obvezu izuzeća od ove zabrane presretanja i prikupljanja podataka o komunikacijama, ali ju je Sud pravde proglasio ništavnim, kao što je navedeno u odjeljku.

Korištenje "kolačića" ("cookies") i drugih nametljivih tehnologija:

Izmijenjena Direktiva o e-privatnosti propisuje, u članku 5. stavku 3., u tehničkoj terminologiji, da države članice moraju osigurati:

> **pohranjivanje informacija ili dobivanje pristupa informacijama koje su već pohranjene, u terminalnoj opremi pretplatnika ili korisnika**, dopušteno je samo pod uvjetom da je dotični pretplatnik ili korisnik dao svoj **pristanak**, budući da je dobio jasne i **sveobuhvatne informacije**, u skladu s Direktivom 95/46 / EZ, između ostalog, o svrhama obrade.

Direktiva pojašnjava u sljedećoj rečenici ovog stavka da:

> To neće spriječiti bilo kakvo tehničko pohranjivanje ili pristup isključivo u svrhu obavljanja prijenosa komunikacije putem elektroničke komunikacijske mreže, ili kao strogo neophodno da bi pružatelj usluge informacijskog društva izričito zatražio od pretplatnika ili korisnika da dostavi usluga.

Imajte na umu da izrazi "*isključivo u svrhu*" i "što je strogo neophodno" naglašavaju da se ova iznimka mora vrlo usko primijeniti.

Izraz "*pohranjivanje informacija ili dobivanje pristupa već pohranjenim informacijama, u terminalnoj opremi pretplatnika ili korisnika*" je tehnički jezik za tehnologije koje dopuštaju da posjetitelj web stranice bude prepoznat od

115 Usp. opsežno tumačenje pojma "korespondencije" u članku 8. EKLJP-a od strane Europskog suda za ljudska prava u poznatom predmetu Klass protiv Savezne Republike Njemačke (presuda od 6. rujna 1978.), par. 41, gdje je Sud smatrao da su "*telefonski razgovori...obuhvaćeni pojmovima "privatnog života" i "korespondencije"[u tom članku]*".

strane web stranice te da ga prati dok koristi web stranicu ili čak preko web stranica. Glavna sredstva koja se koriste za to su takozvani "**kolačići**" - zbog čega je Direktiva iz 2009. koja je ojačala pravila u tom pogledu (kao što je objašnjeno u nastavku) u početku općenito nazvana "**Zakonom o kolačićima**" EU-a i još uvijek ponekad kao takve.

To neće spriječiti bilo kakvo tehničko pohranjivanje ili pristup isključivo u svrhu obavljanja prijenosa komunikacije putem elektroničke komunikacijske mreže, ili kao strogo neophodno da bi pružatelj usluge informacijskog društva izričito zatražio od pretplatnika ili korisnika da dostavi uslugu.

Imajte na umu da izrazi "isključivo u svrhu" i "što je strogo neophodno" naglašavaju da se ova iznimka mora vrlo usko primijeniti.

Zapravo, postoji niz kolačića koji proizlaze iz međunarodnih tehničkih alata poznatih pod nazivom "RFC", usvojenih od strane radne skupine Internet Engineering Task Force (IETF), a koji u svakodnevnoj upotrebi mogu varirati u rasponu od visoko nametljivih "**kolačića za praćenje trećih strana**" do onih koji **nisu nametljivi** i koji poboljšavaju rad internetskih stranica bez praćenja posjetitelja; postoje i druge nametljive tehnologije kao što su **"flash cookies",** HTML5 načini pohrane i takozvani **"evercookies"**.[116] Svi oni spadaju u definiciju "*informacija pohranjenih u terminalnoj opremi*", te se stoga (donekle problematično) sve postupa prema Direktivi o e-privatnosti.[117]

Svrha i značenje članka 5. stavka 3. objašnjeno je jednostavnije u uvodnim izjavama (24) i (25) Direktive o e-privatnosti, u kojoj je jasno navedeno da se proteže i izvan "kolačića". Vrijedi citirati u cijelosti:

> Terminalna oprema korisnika elektroničkih komunikacijskih mreža te informacije pohranjene na takvoj opremi dio su privatnog područja korisnika koje zahtijeva zaštitu prema Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda. Takozvani špijunski programi (***spyware*), mrežne greške (*web bugs*), skriveni identifikatori i druga slična sredstva mogu ući u korisnikov terminal bez njegova znanja s ciljem dobivanja pristupa informacijama, pohranjivanja skrivenih informacija ili ulaženja u trag aktivnostima korisnika te mogu ozbiljno narušiti privatnost korisnika. Uporaba takvih sredstava treba se dopustiti isključivo u legitimne svrhe, uz znanje dotičnih korisnika**. (dodatno naglašeno)
>
> Međutim, takva sredstva, **na primjer takozvani kolačići (cookies)**, mogu biti legitimno i korisno oruđe, na primjer pri analiziranju učinkovitosti dizajna internetskih stranica i oglašavanja te prilikom potvrde identiteta korisnika koji su uključeni u online transakcije. Ako su takva sredstva, na primjer kolačići, namijenjena legitimnoj svrsi, poput olakšavanja pružanja usluga informacijskog društva, njihova uporaba treba se dopustiti pod uvjetom da se korisnicima pruži jasna i precizna informacija, u skladu s Direktivom 95/46/EZ, o svrsi kolačića ili sličnih sredstava kako bi se osiguralo da korisnici budu svjesni informacija koje se stavljaju na terminalnu opremu kojom se služe. Korisnicima treba biti dana mogućnost odbiti pohranjivanje kolačića ili sličnih sredstava na svoju terminalnu opremu. Ovo je posebno važno ako drugi korisnici, a ne izvorni korisnik, imaju pristup terminalnoj opremi te, samim time, i podacima koji sadrže osjetljive privatne informacije pohranjene na takvoj opremi. Informacije o uporabi različitih uređaja koji bi se ugradili na korisnikovu terminalnu opremu, kao i pravo na odbijanje tih uređaja, mogu se ponuditi jednom tijekom iste veze te se također odnose na svaku buduću uporabu tih uređaja do koje može doći tijekom naknadnih veza. Metode davanja informacija, pružanja prava na odbijanje[118] ili zahtijevanje pristanka, trebaju biti što je više moguće pristupačne. Pristup sadržajima posebnih internetskih stranica još uvijek može ovisiti o dobro obaviještenome prihvaćanju kolačića ili sličnoga sredstva, ako se koristi u legitimne svrhe. (dodatno naglašeno)

116 Vidjeti: https://webcookies.org/doc/eu-web-cookies-directive
117 To se može promijeniti u skladu s predloženom novom Uredbom o e-privatnosti, koja bi mogla različito tretirati različite tehnologije u skladu s njihovom relativnom nametljivošću.
118 O zadržavanju prava na odbijanje, vidi sljedeće dvije bilješke.

Glavna promjena koju je donijela Direktiva iz 2002. bila je da se promijenio režim koji pokriva korištenje takvih tehnologija od mjesta gdje je pretplatnik ili korisnik morao biti informiran i dobio "pravo odbiti" postavljanje kolačića (itd.),[119] onaj u članku 5. stavku 3., prema kojem su kolačići dopušteni samo pod uvjetom da je pretplatnik ili korisnik bio ne samo obaviješten, već i dao **pozitivni, izričiti pristanak**, u skladu s uvjetima za (valjanu) suglasnost naveden u glavnoj 1995. Direktive o zaštiti podataka[120] koja je definirala suglasnost kao:

> svaka dobrovoljno dana, posebna i informirana izjava volje, kojom osoba čiji se podaci obrađuju daje svoju suglasnost da se obrade osobni podaci koji se na nju odnose (čl. 2(h)).

Međutim, s obzirom na zamjenu Direktive iz 1995. godine GDPR-om, postavlja se pitanje bi li se sada to trebalo tumačiti kao traženje zahtjevnijeg oblika privole propisanog Uredbom. Ako je to slučaj, privola za postavljanje kolačića i takvih drugih alata sada bi se trebala temeljiti na:

> svako dobrovoljno, posebno, informirano i **nedvosmisleno** izražavanje želja [pretplatnika ili korisnika] kojima on ili ona, **izjavom ili jasnom potvrdom radnjom**, označava pristanak na [postavljanje kolačića ili korištenje drugih alata][121]

Navedeno bi trebalo značiti da upotreba "unaprijed označenih" okvira za uporabu kolačića itd. više neće udovoljavati zahtjevima o suglasnosti iz Direktive o e-privatnosti.

Međutim, još uvijek postoji problem u tome što Direktiva o privatnosti u osnovi tretira sve "kolačiće" i alate za praćenje, bez razlikovanja, recimo, "kolačića sesije" ("session cookies") i "trajnih kolačića" ("persistent cookies").

U praksi, odredba je dovela do kulture "uzmi ili ostavi" na internetu, u kojoj su posjetitelji internet stranica zapravo prisiljeni kliknuti "*Slažem se*" (na postavljanje uobičajenih neodređenih vrsta "kolačića") kako bi pristupili stranici (uključujući čak i mjesta javnih tijela).

SMART studija je utvrdila da:[122]

> pravila o kolačićima i sličnim tehnikama možda nisu u potpunosti postigla svoje ciljeve, s obzirom da korisnici primaju previše poruka upozorenja koje ne razmatraju na odgovarajući način.

Hoće li se to promijeniti novom Uredbom o e-privatnosti tek će se vidjeti, međutim ova pitanja su izravno povezana s primjenom svih temeljnih načela i prava – uključujući ograničenje svrhe, minimiziranje podataka, ograničenje zadržavanja itd. – primjerice, vezano uz pitanja prikladnog razdoblja čuvanja različitih kolačića (ovisno o njihovoj svrsi),[123] vrednovanja pristanka/privole (GDPR pristanak) za upotrebu različitih kolačića, zatim načina na koji subjekti mogu ostvariti svoja prava itd. – te kako se ova pitanja mogu i trebaju implementirati unutar osnova i okvira zaštite podataka – načelo koje je upravo sadržano u GDPR-u.

OGRANIČENJA UPORABE PODATAKA O PROMETU I LOKACIJI

Članak 6. Direktive o e-privatnosti nameće stroga ograničenja kod korištenja i zadržavanja podataka o prometu - i lokaciji od strane pružatelja usluga e-komunikacija. U načelu, **prometni podaci** (tj. podaci

119 U izvornoj verziji iz 2002. prva rečenica članka 5. stavka 3. glasi:

*Države članice osiguravaju da je uporaba elektroničkih komunikacijskih mreža za pohranjivanje informacija ili za pristup informacijama pohranjenim u terminalnoj opremi pretplatnika ili korisnika dopuštena samo pod uvjetom da se dotičnom pretplatniku ili korisniku pruže sveobuhvatne **informacije** u skladu s Direktivom 95/46/EZ, između ostalog o svrhama obrade, te joj se nudi **pravo odbiti** takvu obradu od strane kontrolora podataka.* (dodani naglasci)

120 Ta se promjena ne odražava u uvodnim izjavama navedenim u tekstu, koje nisu izmijenjene u odnosu na izvornu Direktivu iz 2002. godine, i još uvijek se odnose na "pravo na odbijanje", iako je to uklonjeno Direktivom iz 2009. godine. Zapravo, te su riječi postale mrtva slova.

121 Usp. članak 4, stavak 11 GDPR-a. Dodani naglasci.

122 Vidi bilješku 105, iznad.

123 Neke web stranice predviđaju čuvanje podataka u razdoblju od 25 godina, što je zapravo prekomjerno, bez obzira koja je njihova svrha.

obrađeni u svrhu - i potrebni su za - prijenos komunikacije ili za njeno naplaćivanje) mogu se obrađivati i pohranjivati samo od strane pružatelja relevantne usluge e-komunikacija u svrhu ***prijenosa*** e-komunikacije, ***naplaćivanja*** usluge od pretplatnika za komunikaciju, ili da se omoguće ***plaćanja međusobnog povezivanja*** (tj. plaćanja između davatelja za međusobno korištenje mreža) (čl. 1, st. 1 i 2). Ova obrada ne zahtijeva pristanak pretplatnika ili korisnika usluge jer je to potrebno za pružanje usluge. Kada više nisu potrebni za te usluge, moraju biti "izbrisani ili anonimizirani" (čl. 6, st. 1).[124]

Podaci o prometu mogu se koristiti samo svrhu **marketinga elektroničkih komunikacijskih usluga** ili za **pružanje usluga s posebnom tarifom** s **pristankom** pretplatnika ili korisnika. Ponovo, to znači da sada, kada se GDPR u potpunosti primjenjuje, on mora biti u skladu sa zahtjevima GDPR-a za valjanu privolu, tj. da odgovarajuća privola sada mora imati oblik:

> slobodno dane, specifične, informirane i nedvosmislene naznake [pretplatničkih ili korisnikovih] želja po kojima on ili ona, izjavom ili jasnom potvrdom radnjom, označava pristanak na [korištenje svojih podataka o prometu za marketing putem e-pošte] pružatelja komunikacijskih usluga ili pružanja određene usluge s dodanom vrijednošću].

Direktiva o e-privatnosti također propisuje da je davatelj usluge dužan **obavijestiti** pretplatnika ili korisnika svojih usluga o vrstama podataka o prometu koji se obrađuju i o trajanju takve obrade; za obradu na temelju pristanka (tj. za marketing i usluge s posebnom tarifom: vidjeti prethodno u tekstu), ovo pružanje informacija mora se izvršiti **prije dobivanja takvog pristanka** (čl. 6(4)).

Konačno, e-privatnost propisuje da obrada podataka o prometu za pružatelja usluga e-komunikacija za različite **pomoćne svrhe** povezane s pružanjem usluga (**naplata, upravljanje prometom, upiti kupaca, otkrivanje prijevara, marketing i** pružanje **usluga s posebnom tarifom**), od strane zaposlenika, tj. osoblja pružatelja, ili bilo koje osobe koja obrađuje podatke, koju je angažirao pružatelj, mora biti ograničena na osnovi "nužnosti pristupa": svaka od tih osoba trebala bi imati pristup samo takvim podacima o prometu koji su potrebni za obavljanje njihovog specifičnog zadatka (čl. 6(5)). Međutim, "nadležnim [vanjskim] tijelima", kao što su ona koji rješavaju sporove u vezi s plaćanjem ili naplate međusobnog povezivanja, mora se naravno omogućiti pristup podacima o prometu kada je to nužno (čl. 6(6)).

Direktiva o e-privatnosti je čak i stroža u pogledu obrade "**podataka o lokaciji osim podataka o prometu**", tj. (kako je prethodno spomenuto), obrađenih u elektroničkoj komunikacijskoj mreži koji naznačuju ***zemljopisni položaj terminalne opreme korisnika*** (kao što je, uobičajeno, mobilni telefon), ali koji se ***ne obrađuju u svrhe prenošenja e-komunikacije ili naplate takve komunikacije.*** Takvi se podaci mogu jedino obrađivati kad su anonimizirani,[125] ili, u mjeri u kojoj se mogu koristiti za pružanje ***usluge s posebnom tarifom***, s **pristankom** korisnika ili pretplatnika takvih usluga (čl. 9(1), prva rečenica). Pružatelj (davatelj) usluga e-komunikacija mora ponovo **obavijestiti** korisnike i pretplatnike o pojedinostima obrade, prije dobivanja takvog pristanka (*idem*, druga rečenica). Ti korisnici i pretplatnici trebaju štoviše imati mogućnost opoziva takvog pristanaka u bilo koje doba (*idem*, treća rečenica), i/ili privremeno isključiti takvo praćenje lokacije, "na jednostavan način i bez naplate" (čl. 9(2)). I opet, obrada takvih podataka mora biti ograničena na osoblje davatelja usluga e-komunikacija ili pružatelja odgovarajuće usluge s posebnom tarifom (ili osobe koja obrađuje podatke, koju je angažirala bilo koja od tih osoba) (čl. 9(3)).

RAČUN S DETALJNIM ISPISOM

Pretplatnici moraju imati pravo odabrati primati **račune bez detaljnog ispisa** (čl. 8(1), a države članice bi također trebale osigurati drugačije **načine za povećanje privatnosti** u odnosu na račune s detaljnim ispisom (čl. 8(2), tj., račune s detaljnim ispisom koji prikazuju samo pozivne brojeve države ili regije za odlazne

124 O problemima kod anonimizacije takvih podataka, vidjeti diskusiju o tom pitanju u kontekstu GDPR-a, u Drugom dijelu, odlomak 2.1, dalje u tekstu.
125 Vidi prethodnu bilješku (fusnotu).

pozive, ili koji izostavljaju ili prikrivaju posljednje tri znamenke broja koji se zove, kako bi objasnio iznos računa i zaštitio privatnost korisnika (koji možda nije pretplatnik ili član obitelji).

Identifikacija pozivne linije i linije primatelja poziva, te automatsko prosljeđivanje poziva

Davatelji usluga e-komunikacija moraju nuditi i pozivateljima i primateljima poziva (uključujući pozivatelje unutar EU-a [tada EZ-a] koji upućuju pozive trećim državama) **opciju zabrane identifikacije broja pozivatelja**, ali osobe koje primaju poziv s neidentificiranog broja (koji dolazi iz ili izvan EU-a/EZ-a) moraju biti u mogućnosti **blokirati** određeni poziv; i moraju biti u mogućnosti **isključiti** identifikaciju svoje pozivne linije po osnovi pojedinačnog poziva (čl. 8(1) – (4)).

Davatelji usluga e-komunikacija moraju štoviše **obavijestiti javnost** (a naravno posebice svoje pretplatnike i korisnike) o tim opcijama (čl. 8(6)).[126]

Uz primjenu relevantnih nacionalnih propisa, davatelji usluga e-komunikacija mogu **ukinuti blokiranje** identifikacije pozivne linije, ili bilo na zahtjev pretplatnika, ***koji traži ulaženje u trag podmuklim ili zlonamjernim pozivima***, bilo da bi se pružila pomoć, uslugama hitne pomoći i vatrogasne službe, ***u svrhe odgovaranja na takve hitne pozove*** (čl. 10(1) i (2)).

Pretplatnik također mora imati "*mogućnost, na jednostavan način i bez naplate,* ***zaustaviti automatsko prosljeđivanje poziva*** *na pretplatnikov terminal koje obavlja treća osoba*"(čl. 11).

Sve prethodno navedene obvezne/obvezujuće opcije prenesene su u međunarodne tehničke norme, stoga su jednostavno primjenjive u praksi, u odnosu na pametne telefone itd.

Telefonski imenici pretplatnika

Pretplatnici moraju biti informirani o bilo kojoj namjeri uvrštavanja njihovih podataka (tj. njihove fiksne linije ili broja mobilnog telefona) u **telefonski imenik pretplatnika** koji je ili ***javno dostupan*** ili ***mu je omogućen pristup putem usluga upita o podacima iz telefonskih imenika***; te moraju biti u mogućnosti odabrati biti isključeni iz uvrštavanja u takve telefonske imenike (tj., **odlučiti o "ispisu iz telefonskog imenika"**), bez naplate (čl. 12(1) i (2)).[127]

Ova prava vrijede za fizičke osobe – ali države članice također moraju osigurati da su "legitimni interesi pretplatnika koji nisu fizičke osobe [tj. "pravnih osoba", kao što su trgovačka društva]" "na zadovoljavajućoj razini zaštite" u tom smislu (čl. 12(4)).

Ako bi se telefonski imenik koristio za "***bilo koje svrhe … osim traženja kontakt podataka*** *o osobama na temelju njihovog imena te, gdje je to potrebno, minimuma drugih identifikatora*" – npr. ako bi se ti podaci koristili za ***izravnu prodaju, kreditno bodovanje***[128] ili ***vođenje političke kampanje*** – pretplatnike se mora pitati za **dodatni pristanak**, posebno za korištenje njihovih podataka za takve druge svrhe (čl. 12(3)).[129]

126 Te su opcije izvorno izradila nacionalna tijela za zaštitu podataka. Zanimljivo je da su te opcije, za razliku od tehničkih standarda kolačića, čim su usluge identifikacije pozivatelja itd. bile komercijalno ponuđene 1980-ih, integrirane u tehničke međunarodne standarde za telekom prijenos (staromodne fiksne linije), a onda kada su se pojavili mobiteli, u mobilne telefone za aktiviranje opcija. To je bilo zahvaljujući regulatorima Francuske i Njemačke koji su pokrenuli ova pitanja s telekomunikacijskim pregovaračima u Europi, koji su tada potisnuli cjelovita i jednostavna rješenja na globalnoj razini putem GSM normi.

127 U Njemačkoj je naglasak bio na tome da nije potrebno navesti razloge za isključenje iz telefonskih imenika. U Francuskoj je glavno pitanje bila odredba da bi to trebalo biti besplatno. Tijekom pregovora o Direktivi o telekomunikacijama, Francuska je uspjela napustiti cijelu direktivu samo iz tog razloga. Zapravo, nije bio u telefonskom imeniku koji je u to vrijeme vodio do manjeg broja komunikacija - tako manje telekomunikacijskih profita u vrijeme kada su telefonski pozivi plaćeni jedan po jedan - dok je oko 20% pretplatnika tražilo da ne budu u telefonskom imeniku.

128 Usp. tzv. "***red-lining***": praksa davanja drugačijeg tretmana kod iznajmljivanja, kupnje kuće, osiguranja i drugih usluga koje se zasnivaju na podacima o adresi osobe i povijesti navedenih aspekata života – praksa koja je proglašena nezakonitom u SAD-u prije mnogo godina. Vidjeti npr.: https://www.investopedia.com/terms/r/redlining.asp

Također: *How Redlining's Racist Effects Lasted for Decades (Kako su rasistički učinci redlininga trajali desetljećima)*, NY Times, 24. kolovoz 2017. g., dostupno na: https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html (s kartama koje ilustriraju raširenost prakse)

129 Ostaje pitanje vrijedi li isto i za "pravne osobe", s obzirom da ovaj stavak nije spomenut u četvrtom stavku članka 12.

Neželjene komunikacije

Kako je navedeno pod točkom 1.3.2, prethodno u tekstu, Direktiva o zaštiti podataka iz 1995. g. već jamči osobama čiji se podaci obrađuju bezuvjetno **pravo na prigovor** na korištenje bilo kojih osobnih podataka tih osoba za svrhe izravne trgovine (čl. 14(b) Direktive iz 1995. g.). Direktiva o e-privatnosti ovome dodaje zahtjev **prethodnog pristanka** za korištenje ***automatiziranih sustava pozivanja (govorni automati)*** i ***faksimil strojeva (faksovi)***[130] za takve svrhe (čl. 13(1)). Ovaj zahtjev jednako vrijedi i za fizičke i pravne osobe (pojedince i trgovačka društva itd.).

Međutim, ako potrošač pruži kontaktne podatke o elektronskim adresama (telefonski broj ili adrese elektronske pošte itd.) društvu (tvrtki) u kontekstu prodaje proizvoda ili usluge, prodavatelj može koristiti te podatke

za **marketing svojih sličnih proizvoda ili usluga** takvom potrošaču (tzv. "***proximity marketing***"), pod uvjetom da se potrošaču omogući jednostavan način prigovora na takav način marketinga (tj. osim ako se nudi opcija odustanka, tj. "***opt-out***") (čl. 13(2)).

U pogledu ostalih oblika izravne trgovine (tj. izravni marketing koji nije "*proximate*" izravni marketing uz korištenje drugih sredstava osim automatiziranih govornih automata ili telefaks strojeva), države članice mogu **odabrati** između prethodnog pristanka ("***opt-in***" ili pristanak na neku opciju) i modela ("informiran, ali nije prigovorio") "***opt-out*"/"odustanka"** (čl. 13(3)).[131] Međutim, slanje elektronske pošte u svrhe izravnog marketinga "pri čemu se maskira ili krije identitet pošiljatelja u čije se ime komunikacija provodi, odnosno bez valjane adrese na koju primatelj može poslati zahtjev za prestankom takvih komunikacija", mora uvijek biti zabranjeno (čl. 13(4)).

Izuzeća i ograničenja (derogacije):

Članak 15. Direktive o e-privatnosti jasno propisuje da države članice mogu ograničiti različita prava i obveze nametnute direktivom, po istoj osnovi široko definirane klauzule "**važnog javnog interesa**" o izuzeću, sadržane u glavnoj Direktivi o zaštiti podataka iz 1995. g. (čl. 13), tj. "*kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite **nacionalne sigurnosti** (odnosno državne sigurnosti), **obrane, javne sigurnosti** te s ciljem **sprečavanja, istrage, otkrivanja i progona kaznenih djela***" – čemu Direktiva o e-privatnosti jedino još dodaje: "*odnosno **neovlaštene uporabe elektroničkog komunikacijskog sustava***". Podvučene riječi još su dodatno naglašene u Direktivi o e-privatnosti dodavanjem izričite klauzule, koja glasi:

> Sve mjere iz ovog stavka moraju biti u skladu s općim načelima prava Zajednice, uključujući onima iz članka 6. stavaka 1. i 2. Ugovora o Europskoj uniji (čl. 15(1), posljednja rečenica)

Članci iz UEU-a, na koje se odredba poziva, odnose se na Povelju o temeljnim pravima EU-a (objavljenu 2000. g., tj. nakon stupanja na snagu Direktive o zaštiti podataka iz 1995. g.), odnosno na Europsku konvenciju o ljudskim pravima.

Premda je ovo dobrodošlo izričito priznanje ključnog, euro-ustavnog zahtjeva poštivanja temeljnih prava i sloboda, ipak to zapravo nije novost: dotična načela vladavine prava bila su u praksi (i u pravnim instrumentima) već primijenjena također i u doba usvajanja "majke" Direktive, u sintagmi "općim načelima prava Zajednice".[132]

Članak 15(1) također propisuje da, u cilju zaštite različitih navedenih "važnih javnih interesa", ali uz primjenu ključnog *upozorenja* o poštivanju ljudskih prava i općih načela prava Zajednice:

130 "Faksimil" ili "faks" je uređaj koji omogućuje slanje slike (često slike dokumenta) putem telefonske mreže. U današnje je vrijeme korištenje tih uređaja rijetko. Vidjeti: https://faxauthority.com/fax-history/

131 EU "*opt-out*" model traži obavještavanje osobe čiji se podaci obrađuju o sljedećem: (i) namjeri korištenja podataka te osobe za izravni marketing; (ii) njihovo pravo odustati ("*opt-out*") od takvog marketinga; i (iii) pojedinosti o tome kako (na jednostavan način i bez naplate) ostvariti ovo pravo. Zamijetite da se europski "opt-out" model bitno razlikuje od američkog modela koji ne traži obavještavanje osoba čiji se podaci obrađuju o bilo kojim od tih pojedinosti.

132 Vidjeti bilješku (fusnotu) 66, prethodno u tekstu.

Države članice mogu, *između ostalog*, donijeti zakonske mjere kojima se omogućuje **zadržavanje podataka tijekom ograničenog razdoblja** opravdano razlozima određenim u ovom stavku (članak 15(1), druga rečenica).

Ovaj izvorni tekst, sa svojim **eksplicitnim pravilom o ograničenjima zakona, učinkovito zabranjujući neselektivno zadržavanje podataka**, važan je u smislu naknadnih pokušaja europskog zakonodavca da nametne upravo takve obveze neselektivnog zadržavanja podataka sukladno tzv. Direktivi o zadržavanju podataka, koju je u konačnici Sud Europske unije proglasio nevaljanom, o čemu se govori pod točkom 1.3.4, u nastavku.

Nadzor i provedba

Dok su Direktivu o zaštiti podataka iz 1995. godine provodili stručnjaci, neovisna tijela za zaštitu podataka, a te iste vlasti provode GDPR, države članice EU-a mogle bi odlučiti da nadzor i provedbu Direktive o e-privatnosti stave u ruke drugom tijelu ili ruke različitih tijela. To je dovelo do dodjele nadzora različitim tijelima u odnosu na različita pitanja obuhvaćena Direktivom o e-privatnosti u državama članicama.

Komisija je utvrdila da "dodjela nadležnosti za provedbu širokom rasponu nadležnih tijela koja se često preklapaju" također "[otežavala] učinkovitost pravila u prekograničnim slučajevima".

Primjena drugih glavnih elemenata Direktive o zaštiti podataka iz 1995. g.:

Konačno, u ovom pregledu pravila iz Direktive o e-privatnosti, treba zamijetiti da Direktiva o e-privatnosti izrijekom propisuje da će se zahtjevi propisani Direktivom iz 1995. g. po pitanju **pravnih lijekova, odgovornosti i sankcija** (opisano prethodno, pod točkom 1.3.2) također primjenjivati i u odnosu na Direktivu o e-privatnosti (čl. 15(2)); te da će **Radna skupina članka 29.** (također opisano pod tom točkom) provoditi svoje zadaće kako je propisano u Direktivi iz 1995. g., također i u odnosu na Direktivu o e-privatnosti (čl. 15(3)); te da države članice moraju predvidjeti "učinkovite, proporcionalne i odvraćajuće" kazne za kršenje Direktive (čl. 15a).

1.3.4 Instrumenti zaštite (ili zaštitni instrumenti) trećeg stupa[133]

U razdoblju od sredine 1990-ih do 2009. godine, u Europskoj uniji uspostavljen je značajan broj tijela čija je svrha olakšati suradnju između država članica u području policije i kaznenog prava (pravosuđe i unutarnji poslovi ili PUP) – tzv. treći stup Europske unije[134] - koja su usredotočena na uspostavljanje paneuropskih baza osobnih podataka kao i pravila i procedura za pristup tim bazama te razmjenu osobnih podataka između samih država članica.

Navedeno uključuje Europol (1998), Schengenski informacijski sustav – SIS-I (2001, dopunjen SIS II 2013. godine), Eurojust (2002), Eurodac (2003), Vizni informacijski sustav – VIS (2004) te Carinski informacijski sustav – CIS (2009).

U prethodnom razdoblju, Vijeće je usvojilo 123 instrumenta u području pravosuđa i unutarnjih poslova – PUP).[135] Godine 2005., sedam država članica potpisalo je Prumsku konvenciju te je Odlukom od 23. lipnja 2008. godine Europsko Vijeće odlučilo integrirati ključne odredbe te Konvencije u pravni okvir EU-a, kako bi

se omogućila šira razmjena (između zemalja članica EU) biometrijskih podataka (DNA i otisci prstiju) u svrhu suzbijanja terorizma i prekograničnog kriminala.

133 Pojedinosti o zakonu iz ovog područja dostupne su u povijesnim dijelovima odgovarajućih poglavlja u: Steve Peers, (2016). EU Zakon o pravosuđu i unutarnjim poslovima: Volume I: EU Zakon o imigracijama i azilu (Četvrto izdanje) te Volume II: EU Kazneno pravo, policijsko i građansko pravo (četvrto izdanje), oba Oxford University Press, 2016.
134 Vidi bilješku 58, iznad.
135 Vidi Emilio De Capitani, *Metamorphosis of the third pillar: The end of the transition period for EU criminal and policing law, EU Law Analysis blogspot,* 10 July 2014, dostupan na: https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html

Također, 2008. godine Vijeće je donijelo Okvirnu odluku s ciljem uspostave zajedničkih načela zaštite osobnih podataka u području pravosuđa i unutarnjih poslova (PUP).[136] Međutim, iako su mnoga pravila sadržana u Okvirnoj direktivi donesena temeljem Direktive 95/46/EC i Konvencije Vijeća Europe, kao tadašnji Europski nadzornik za zaštitu osobnih podataka, Peter Hustinx, istaknuo je sljedeće: "razina zaštite bila je mnogo niža s obzirom na opseg i sadržaj".[137] Što se tiče opsega, autor je naveo sljedeće:[138]

> Odluka se primjenjuje jedino u slučaju kada se osobni podaci prenose ili ustupaju drugim državama članicama, slijedom čega se ne odnosi na "nacionalnu" obradu (npr. prilikom obrade od strane ili u državi članici), za razliku od same Direktive 95/46/EZ.

Nakon stupanja na snagu Lisabonskog ugovora, 2009. godine, koje je ujedno okončao strukturu "tri stupa",[139] započelo je petogodišnje prijelazno razdoblje, tijekom kojeg je zakonodavni okvir, koji se odnosio na područje pravosuđa i unutarnjih poslova trebao biti prenesen unutar nadnacionalnog zakonodavnog okvira Europske unije (vidi odjeljak 1.4.2, ispod).[140] Međutim, 2018. godine Okvirna odluka 2008 zamijenjena je novom Odlukom

1.3.5 Zaštita podataka u drugom stupu (ili Zaštita podataka drugog stupa)

Neformalni sustav za "Europske političke suradnje" (EPC) za vanjska pitanja djelovao je 1970. - 1993. Ugovorom iz Maastrichta, koji je stupio na snagu 1993. godine, ovo pitanje bilo je definirano kao "Zajednička vanjska i sigurnosna politika" (ZVSP) – europski drugi stup. Međutim, do daljnjeg razvoja ZVSP-a temeljenog na Lisabonskom ugovoru 2009. (čime je ukinuta struktura "stupova"),[141] kako je pojašnjeno u odlomku 1.4.4 u nastavku, nisu postojala posebna pravila o zaštiti podataka koja su se primjenjivala na obradu osobnih podataka u ovom području (izuzev nacionalnih zakona o zaštiti podataka zemalja članica i Konvencije Vijeća Europe).

1.3.6 Zaštita podataka za institucije EU

Prvotno nisu postojala nikakva sveobuhvatna ili dosljedna pravila o zaštiti podataka primjenjiva na institucije EU, sve do 2001. kada su Uredbom (EZ) 45/2001 po prvi put uvedena pravila na temelju čl. 286 Ugovora o EU, koji je zahtijevao takva pravila.[142]

Pravila o zaštiti podataka sadržana u Uredbi 2001. temeljena su na tada postojećim pravilima o zaštiti podataka Zajednice koja su primjenjivale države članice, posebno Direktivi o zaštiti podataka 1995. te Direktivi o e-privatnosti 2002.

Uredbom 45/2001 je također uspostavljena i institucija Europskog nadzornika za zaštitu podataka, kao neovisnog nadzornog tijela čija je odgovornost praćenje obrade osobnih podataka od strane institucija i tijela Zajednice te je zahtijevano imenovanje službenika za zaštitu podataka svake pojedinačne institucije ili tijela.

Uredba (EZ) 45/2001 ukinuta je Uredbom (EU) 2018/1725, koja je stupila na snagu 11. prosinca 2018., kako je pojašnjeno u odlomku 1.4.5 u nastavku.

---

136 Okvirna odluka Vijeća 2008/977/PUP od 27. studenog 2008 o zaštiti osobnih podataka u okviru suradnje između policije i pravosuđa u kaznenim pitanjima, OJ L 350, 30. prosinca 2008., p. 60, dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977

137 Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p. 15, dostupno na: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

138 Idem, vezano uz Uvodnu izjavu (7) i čl. 1 Okvirne odluke.

139 Vidi bilješku 58, iznad.

140 Vidi Protokol 36 Lisabonskog ugovora i Emilio De Capitani, o.c. (bilješka 141, iznad)

141 Vidi bilješku 58, iznad.

142 Uredba (EZ) 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000 o zaštiti pojedinaca u vezi obrade osobnih podataka od strane europskih institucija i tijela te o slobodnom kretanju takvih podataka, OJ L 8, 12. siječnja 2001., p. 1-22, dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

1.4 ZAKONODAVNI OKVIR O ZAŠTITI PODATAKA ZA BUDUĆNOST

Do kraja prvog desetljeća 21. stoljeća, postalo je posve jasno da instrumenti o zaštiti podataka koji u bitnome datiraju iz 20. stoljeća, o čemu se govori u odlomku 1.3, prethodno u tekstu, više ne odgovaraju svrsi: oni su zamišljeni i izrađeni prije masovnog pristupa internetu (ili barem globalnom informacijskom sustavu, tzv. world-wide webu), sveprisutnog (i mobilnog) računarstva, prije "Big Data", prije sveopće internetizacije ("Internet of Things", IoT), dubinskog profiliranja, algoritamskog donošenja odluka i umjetne inteligencije ("Artificial Intelligence", AI). I u samom EU-u i u Vijeću Europe, zbog toga su pripremljeni novi ili ažurirani ("modernizirani") instrumenti o zaštiti podataka, o čemu se govori u ovom odlomku.

1.4.1 EU Opća uredba o zaštiti podataka

Europska je komisija 2012. godine predložila usvajanje Opće uredbe o zaštiti podataka (GDPR)[143] kako bi udovoljila izazovima koje su postavile nove tehnologije i nove usluge.

Zamislila je jednu snažnu zaštitu podataka na visokoj razini kao temeljni uvjet za stjecanje povjerenja u internetsku (*online*) okolinu, što je samo po sebi "*presudno za gospodarski razvoj*"; novi, ažurirani *lex generalis* režim zaštite podataka trebao je odigrati "*glavnu ulogu u*

Digitalnoj agendi za Europu (the Digital Agenda for Europe), te općenitije u Strategiji Europa 2020 (the Europe 2020 Strategy)".[144]

Pozadina, pravni položaj i pristup, kao i ključni elementi GDPR-a podrobno su opisani u Drugom dijelu ovog priručnika. Ovdje je dovoljno zamijetiti da GDPR značajno **proširuje i ojačava glavna načela i pravila; izravno dodaje genetske i biometrijske podatke na listu osjetljivih podataka (što je inspirirano radom na "moderniziranoj" Konvenciji o zaštiti podataka Vijeća Europe, pojašnjenoj ispod, u 1.4.3);** ima za cilj dovesti do **veće usklađenosti** prava zaštite podataka u državama članicama EU-a (barem u područjima gdje se primjenjuje, što je općenito područje prethodno zvano "prvi stup" Europskih zajednica), sukladno važnoj novoj sudskoj praksi Europskog suda – premda uz primjenu širokog raspona "*klauzula sa specifikacijama*" (npr. odredbe koje prepuštaju zakonodavstvu država članica detaljnije definiranje određenih pitanja, a sve u okviru GDPR-a, ugovora Europske unije kako ih tumači SEU te nacionalnog ustavnog i općeg pravnog sustava[145]; omogućava **jača (i neka nova) prava ispitanika;** omogućava **bliskiju prekograničnu suradnju** između nadzornih tijela za zaštitu podataka (TZP-ova) država članica; i trebala bi dovesti do **bolje, dosljednije primjene i provedbe** pravila.

Točnije, kako je već navedeno u Uvodu u ovaj priručnik, GDPR uvodi (ili barem, specificira) **načelo "pouzdanosti" ["odgovornosti"] – danas temeljno i obvezno u svim državama članicama**, a u mnogo slučajeva (uključujući u odnosu na sva javna tijela na koja se primjenjuje Uredba) **obvezuje** na osnivanje institucije, **po voditelju obrade ili izvršitelju imenovanih, službenika za zaštitu podataka** (**SZP-ova**).

Kako je dalje u tekstu objašnjeno u Drugom dijelu, ovo je dvoje povezano: sukladno GDPR-u, SZP-ovi će biti osobe koje će u praksi morati osigurati poštivanje načela "pouzdanosti" ["odgovornosti"] od strane organizacija kojima pripadaju, odnosno unutar tih organizacija.

---

143 Prijedlog Europske komisije: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25. 01. 2012, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
U isto doba, Komisija je predložila i odvojeni instrument o zaštiti podataka, prijedlog Proposal for a Directive on "the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data," (COM(2012) 10 final) – ali o toj se direktivi ne govori u ovom priručniku (vidjeti bilješku u okviru pod naslovom "*O ovom priručniku*", na str. 1 priručnika).

144 Prijedlog GDPR-a/Proposal for a GDPR (prethodna bilješka (fusnota)), str. 1-2 (s referencama na glavne dokumente o Digitalnoj agendi i Strategiji Europa 2020.). Nasljednik Digitalne agenda je Strategija jedinstvenog digitalnog tržišta ("*DSM Strategy*").

145 Vidi Drugi dio, odjeljak 2.2, ispod, pod podnaslovom "...ali s klauzulama sa specifikacijama ili klauzulama o specifikacijama".

1.4.2 Predložena Uredba EU o e-privatnosti

Premda je, kako je navedeno u ranijim dijelovima teksta, jedan od glavnih ciljeva predloženog GDPR-a bio pozabaviti se izazovima koji su se javili zbog **manjka povjerenja (posebice, povjerenja potrošača) u *online* okolinu**, Komisiji je trebalo još pet godina da predloži novi instrument za zamjenu pravila koja su upravo ponajviše relevantna za tu okolinu, tj. Direktivu o e-privatnosti (Direktiva 2002/58/EZ), o kojoj se govori pod točkom 1.3.4, prethodno u tekstu (koja stoga ostaje na snazi donekle ostavljena kao "siroče").

Ovo se dogodilo u obliku prijedloga koji je objavljen u siječnju 2017. g., kako bi se zamijenila Direktiva o e-privatnosti, također uredbom, dakle **prijedlogom Uredbe o e-privatnosti**.[146]

Prijedlog je i dalje u ranim fazama zakonodavnog procesa: u doba pisanja ovog teksta (kolovoz 2018.), o njemu se i dalje raspravlja interno unutar Vijeća) i uz posvećivanje mnogo pažnje od strane oba predlagatelja (grupe za građanska prava, grupe potrošača i grupe za digitalna prava)[147] i oponenata (uključujući neke od glavnih američkih internetskih giganata, tzv. "*Internet Giants*", koji traže potpuno povlačenje prijedloga ili njegovo značajno "razvodnjavanje").[148] Stoga je doista prerano ovdje detaljnije raspravljati o predloženoj uredbi: nesumnjivo, finalna verzija će se barem u nekim vidovima vjerojatno prilično razlikovati od prijedloga.

Stoga će morati biti dostatno, za ovo prvo izdanje priručnika, jednostavno izložiti **ključne točke prijedloga Komisije**, kako je to Komisija sama predstavila:[149]

> Prijedlog za uredbu o pravilima o privatnosti na visokoj razini za sve elektroničke komunikacije uključuje:
>
> - **Nove igrače:** pravila o privatnosti [*i zaštiti podataka*] u budućnosti će se također primjenjivati na nove [*tzv. "Over-The-Top" ili OTT*] igrače koji pružaju usluge elektroničkih komunikacija, kao što su WhatsApp, Facebook Messenger i Skype. Ovo će osigurati da ove popularne usluge jamče istu razinu povjerljivosti komunikacija kao i tradicionalni telekom operateri.
> - **Jača pravila:** sve osobe i poduzeća u EU uživat će istu razinu zaštite njihovih elektroničkih komunikacija putem ove izravno primjenjive uredbe. Poduzetnici će također imati koristi od jednog jedinog kompleta pravila diljem cijelog područja EU-a.[150]
> - **Sadržaj komunikacija i meta-podataka:** privatnost se jamči za sadržaj komunikacija i meta-podataka, tj. vrijeme poziva i lokacija. Metapodaci imaju komponentu visoke privatnosti i treba ih anonimizirati ili izbrisati ako korisnici nisu dali svoju privolu, osim ako su podaci potrebni za naplatu usluge.[151]
> - **Nove poslovne mogućnosti:** kad je jednom privola dana za komunikacijske podatke – sadržaj i/ili metapodatke – tradicionalni telekom operateri će imati više mogućnosti za pružanje dodatnih usluga i za razvijanje svojeg poslovanja. Primjerice, mogli bi proizvesti toplinske mape koje navode prisutnost pojedinaca; to bi moglo pomoći javnim tijelima i kompanijama prijevoznicima kod razvoja novih infrastrukturnih projekata.
> - **Jednostavnija pravila o kolačićima (*cookies*):** odredba o kolačićima, koja je dovela do preopterećenja zahtjeva za privolom korisnika interneta, bit će osuvremenjena. Novo će pravilo biti više prilagođeno korisniku (*user friendly*) s obzirom da će postavke pretraživača omogućavati jednostavan način za prihvaćanje ili odbijanje kolačića za praćenje i drugih identifikatora. Prijedlog također pojašnjava da nije potrebna nikakva privola za kolačiće koji ne narušavaju privatnost, ali poboljšavaju internetsko

146 Prijedlog Uredbe Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, Brussels, 10.01.2017, dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

147 Vidjeti Otvoreno pismo europskim državama članicama o reformi e-privatnosti / Open letter to European member states on the ePrivacy reform, koje je poslala velika grupa nevladinih organizacija 27. ožujka 2018. g., dostupno na: https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf

148 Vidjeti: Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council*, 4. lipnja 2018. g., dostupno na: https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targetscouncil

149 https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

150 Ali primijetite da će ovo ovisiti o pravilima u Uredbi o e-privatnosti, koja ne sadrži "fleksibilne"/specifikacijske klauzule, kakve su sadržane u GDPR-u (vidjeti Drugi dio, odlomak 2.1, dalje u tekstu). Ako bi finalni tekst Uredbe o e-privatnosti sadržavao takve "fleksibilne" odredbe (što je vrlo vjerojatno), bilo bi od ključne važnosti – posebno za *online* okolinu, koja je po svojoj prirodi transnacionalna – dodati odredu o "mjerodavnom pravu".

151 Ali primijetite kontinuirane napore država članica i Komisije da zadrže ili ponovno uvedu obvezno zadržavanje (meta)podataka e-komunikacija: vidjeti odlomak 1.3.4, prethodno u tekstu.

iskustvo (npr. pamćenje povijesti kupovine) ili kolačići koje koristi internetska stranica za brojanje broja posjetitelja.

- **Zaštita od neželjene pošte (*spam*):** ovaj prijedlog zabranjuje neželjene elektroničke komunikacije putem elektronske pošte, SMS-a i automatiziranih glasovnih uređaja. *Ovisno o nacionalnom pravu,* osobe će biti zaštićene beziznimno (po pravilu) ili će moći koristiti popis zabranjenih poziva (*do-not-call list*) kako ne bi primali marketinške telefonske pozive.[152] Pozivatelji koji se bave marketingom trebat će prikazati svoj broj ili koristiti poseban pozivni broj koji ukazuje na marketinški poziv.
- **Učinkovitija provedba:** provedba pravila o povjerljivosti u Uredbi bit će odgovornost tijela za zaštitu privatnosti, koja su već nadležna za pravila sadržana u Općoj uredbi o zaštiti privatnosti.

1.4.3 Provedba Direktive o zaštiti podataka iz 2016. (LED)

UVOD

Člankom 10. stavkom 1. Protokola 36 Lisabonskog ugovora iz 2009. predviđeno je prijelazno razdoblje prije potpune primjene ovlasti Komisije i Suda na europske pravne dokumente u području policijske i pravosudne suradnje u kaznenim pitanjima, usvojene prije stupanja na snagu Lisabonskog ugovora (prethodna stečevina trećeg stupa). Ovo prijelazno razdoblje završilo je 1. prosinca 2014. godine.

U 2012. godini, Komisija je podnijela prijedloge direktive koja se odnosi na ovo područje, zajedno s prijedlogom Opće uredbe o zaštiti podataka (predstavljena u odlomku 1.4.1, iznad te detaljnije prikazana u Drugom dijelu ovog priručnika).[153] Međutim, kao i GDPR, Direktiva (EU) 2016/680 – zaštita pojedinaca u vezi s obradom njihovih osobnih podataka od strane policije ili tijela kaznenog prava i o slobodnom kretanju takvih podataka (također poznata kao "Direktiva o provedbi zakona", LED, "Policijska direktiva o zaštiti podataka" ili samo "Policijska direktiva") usvojena je tek 2016. godine, istog dana kao i GDPR.[154] Za razliku od GDPR-a koji je kao Uredba izravno primjenjiv u pravnom poretku država članica (iako, u tom slučaju, uz značajan broj klauzula koje zahtijevaju daljnju specifikaciju unutar nacionalnog zakonodavstva)[155], LED se ne primjenjuje izravno (tj. nema izravnog utjecaja) već mora biti prenesen u nacionalno zakonodavstvo. Navedeno mora biti provedeno u roku dvije godine od trenutka stupanja direktive na snagu, tj. do 6. svibnja 2018. (nekoliko tjedana prije pune primjene GDPR, 25. svibnja 2018. godine).

Potrebno je istaknuti kako su opširna duža razdoblja implementacije predviđena člancima 61 – 63 Direktive, s obzirom na različite okolnosti velikog broja postupaka obrade podataka, a o čemu će biti riječi na kraju ovog odlomka o LED-u, pod naslovom "Odgoda prijenosa".

Ovdje je potrebno istaknuti glavne karakteristike i zahtjeve LED-a. [156]

DIREKTIVA UMJESTO OKVIRNE ODLUKE VIJEĆA

Prvenstveno je potrebno istaknuti kako postavljanje pravila za obradu osobnih podataka direktivom predstavlja značajan napredak u odnosu na njihov sadržaj u Okvirnoj odluci Vijeća kao što je ona iz 2008., koja je ukinuta stupanjem na snagu LED-a.[157] Kao direktiva, dostupna je nacionalnim sudovima koji se na istu mogu

152 Ovo je upravo takva "fleksibilna" odredba, kako je spomenuto u bilješci (fusnoti) 120, prethodno u tekstu – i ilustrira potrebu za pravilom o "mjerodavnom pravu" kako bi se razjasnilo koje od različitih nacionalnih prava primijeniti u slučaju prekograničnih marketinških komunikacija.
153 Vidi bilješku 149, iznad.
154 Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL L119, 04. svibnja 2016, p. 89-131, dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG
Direktiva je formalno ušla u primjenu dan nakon objave u Službenom listu, 5. svibnja 2016. – ali kao što je navedeno u tekstu, postala je obvezujuća (uklapanjem u nacionalno zakonodavstvo država članica) dvije godine kasnije, točnije 6. svibnja 2018. godine.
155 Vidi Drugi dio, odjeljak 2.2., ispod.
156 Kako je objašnjeno na početku Priručnika, naša namjera je proširiti EU pravo zaštite podataka izvan GDPR-a u drugom izdanju. To bi se posebno proširilo pravilima LED-a koja su ovdje sažeta.
157 Vidi Steve Peers, *The Directive on data protection and law enforcement: A Missed Opportunity?,* Statewatch Analysis blog, April 2012, dostupno na: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf

pozvati (pa tako i Sud pravde) u pojedinačnim postupcima protiv države te isto tako podliježe izvršnoj ovlasti Komisije, koja za cilj ima osigurati instrumente kako bi se ista pravilno prenijela u nacionalno zakonodavstvo.

Područje primjene LED-a

i. Obuhvaćene aktivnosti

U odnosu na područje primjene LED propisuje sljedeće:

Područje primjene

1. Ova Direktiva primjenjuje se na obradu osobnih podataka od strane nadležnih tijela [u svrhu sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu i sprječavanje prijetnji javnoj sigurnosti.
2. Ova Direktiva se primjenjuje na obradu osobnih podataka koja se u cijelosti ili djelomično obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji su dio sustava pohrane ili su namijenjeni da postanu dio sustava pohrane.-
3. Ova Direktiva se ne primjenjuje na obradu osobnih podataka:
   a) tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije
   b) koju obavljaju institucije, tijela, uredi i agencije Unije.[158]

Potrebno je unutar "nadležnog tijela" jasno odrediti granicu između subjekata obrade podataka na koje se primjenjuju odredbe LED-a te subjekata obrade na koje se primjenjuju odredbe GDPR-a, a sve uzimajući u obzir Uvodnu izjavu (12). Navedena uvodna izjava, posebno u zadnjoj rečenici, ističe kako je obrada osobnih podataka u odnosu na "*druge zadaće*" povjerene nadležnom tijelu, a koje se "ne provode nužno u svrhu sprječavanja, istrage, otkrivanja ili progona kaznenih djela, uključujući zaštitu i sprječavanje prijetnji javnoj sigurnosti, prvenstveno u nadležnosti GDPR-a, a ne LED-a.

Voditelj obrade mora s posebnom pažnjom razgraničiti prethodno spomenuta pitanja vezana uz nadležnost LED-a i GDPR-a. Također, važno je odrediti jesu li i ostala pitanja kao što su opseg prikupljanja i daljnje obrade osobnih podataka vezanih za "incidente" kada nije potpuno jasno je li počinjen prekršaj te pitanja vezana za poduzimanje mjera (uključujući i "*korektivne mjere*") prilikom demonstracija ili velikih sportskih događanja koja posljedično "*mogu dovesti do počinjenja određenih prekršaja*" (ili ne), u nadležnosti LED-a. Svi odgovori na postavljena pitanja od velikog su značaja za razinu zaštite osobnih podataka koja treba biti osigurana, npr. u smislu informiranja ispitanika/građana, ograničenja zadržavanja podataka, ograničenja prava ispitanika/građana itd. U međuvremenu, službenici za zaštitu podataka koji rade unutar nadležnih tijela trebali bi pomoći relevantnim tijelima pri izradi ovih odluka, a sve s ciljem osiguranja prikladne razine zaštite podataka općenito.

Koncept "javna sigurnost" često se koristi u kontekstu iznimaka od EU prava, tj. kako bi se naznačili razlozi koji se mogu koristiti za opravdanje aktivnosti koje bi inače bile u suprotnosti s pravom Unije. Kao što Koutrakis ističe: "Javna sigurnost predstavlja temelj za izuzeće u odnosu na sve četiri slobode sukladne osnovnim pravilima Unije."[159] U Izvješću nastalom na zahtjev IMCO Odbora Europskog parlamenta navedeno je:[160]

> Od svih osnova za izuzeće od slobodnog kretanja, javna sigurnost je najsličnija onome što se tradicionalno shvaća kao srž nacionalnog suvereniteta, odnosno područje aktivnosti koje su sastavni dio odgovornosti države u odnosu na zaštitu teritorija i građana (dodatno naglašeno).

158 Obrada od strane EU tijela, ureda i agencija u svrhu sprječavanja, otkrivanja, istrage i progona kaznenih djela propisana je posebnim pravilima, sadržanim u Poglavlju IX nove regulative o obradi osobni podataka od strane EU institucija (itd.), Uredbom (EU) 2018/1725, koja se spominje u pododlomku 1.4.5, niže u tekstu.

159 Panos Koutrakis, Public Security Exceptions and EU Free Movement Law, in: Koutrakos, P., Nic Shuibhne, N. and Sypris, P. (Eds.), Exceptions from the EU Free Movement Law, 2016 (pp. 190-217), p.2, dostupno na: http://openaccess.city.ac.uk/16192/ (Vezano za čl. 36 (Dobra), 45(3) i 52 (Osobe), 62 (Usluge) i 65 TFEU (Kapital)).

160 Iznimka javne sigurnosti u području neosobnih podataka u Europskoj uniji, Izvješće nastalo na temelju zahtjeva IMCO odbora Europskog parlamenta pripremljeno od strane Kristina Irion, PE 618.986, Travanja 2018, p. 3, dostupno na: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618986/IPOL_BRI(2018)618986_EN.pdf

Najvažnija presuda Suda Europske unije po pitanju javne sigurnosti je ona donesena u slučaju *Campus Oil*[161], kojom je Sud presudio da je nacionalna mjera – u slučaju nacionalne kvote za opskrbu rafiniranom naftom Republike Irske - bila opravdana jer rafinirana nafta ima:

temeljnu važnost za opstanak određene države i to ne samo za njezine usluge nego i za svoje institucije u cijelosti, važne javne usluge kao i za preživljavanje njezinih građana (stavak 34, dodatno naglašeno).

Iz navedenog je jasno kako, s jedne strane, pojam "javne sigurnosti" upotrebljavan unutar EU prava nije ograničen samo na pitanja koja se odnose na kriminalne aktivnosti, već je njegov opseg proširen na pitanja kao što su zaštita "temeljnih javnih usluga" te mjera koje za cilj imaju osiguravanje "opstanka (stanovnika) zemlje"; međutim, s druge strane, pojam nema toliko širok opseg kao "javni red" – pojam koji se često koristi u policijskom pravu za pitanja kao što su osiguravanje mira prilikom demonstracija, skupova i proslava.162 Umjesto toga, kao što to Vijeće ističe, pitanje koje je potrebno štititi mora se odnositi na:[163]

istinsku i dovoljno ozbiljnu prijetnju koja ugrožava jedno od temeljnih interesa društva, kao što je prijetnja funkcioniranju institucija i osnovnih javnih službi te opstanku društva, a isto tako i rizik od ozbiljnog poremećaja vanjskih odnosa ili mirnog suživota nacija ili rizik u pogledu vojnih interesa.

Određivanje preciznih granica toga što je obuhvaćeno (kriminalnim) prijetnjama javnoj sigurnosti postavlja složena pitanja procjene u posebnim okolnostima. Postavlja se pitanje kada javni nered – npr. prekid letova zbog prosvjeda protiv protjerivanja tražitelja azila – predstavlja prijetnju ključnoj javnoj usluzi?[164] Također, kada je rizik od "povrede vanjskih odnosa" – primjerice, prosvjeda protiv državnog posjeta predsjednika određene države – potencijalno opasan da bi se mogao klasificirati kao opasnost za javnu sigurnost? Upravo odgovori na ova pitanja određuju primjenjuje li se LED na bilo kakvu obradu osobnih podataka povezanih s ovim radnjama.

Dok mnogi subjekti –-osobito oni iz javnog sektora kao što su lokalne vlasti ili tijela koja se bave pitanjima zaštite okoliša, socijalne skrbi ili zaštite životinja – imaju određene javne ovlasti i moći povezane sa (određenim) zločinima i (određenim) prijetnjama javnoj sigurnosti, glavne zadaće tih tijela neće biti povezane s istragom kaznenih djela unutar njihovih relevantnih nadležnosti, niti s prijetnjama javnom redu (bilo da se radi o zločinima ili ne).

Službenici za zaštitu podataka u javnim tijelima bi trebali pažljivo ispitati u kojoj mjeri se obrada osobnih podataka od strane njihove organizacije ili organizacija može promatrati u okviru GDPR-a, a u kojoj mjeri je ona regulirana LED-om. Navedeno neće uvijek biti jednostavno objasniti i službenici za zaštitu podataka bi trebali na tome raditi zajedno s voditeljem obrade, relevantnom pravnom službom te nadležnim nadzornim tijelom. Nadalje, osobni podaci obrađeni u postupcima obrade koji podliježu LED-u morat će se čuvati odvojeno od osobnih podataka obrađenih u postupcima obrade koji podliježu GDPR-u, uz posebna pravila i politike o tome kada se osobni podaci iz određene kategorije/za određenu svrhu mogu koristiti u okviru druge kategorije/za drugu svrhu.[165]

Konačno, postavlja se pitanje u vezi s granicom između aktivnosti članica EU u području "sprječavanja, istrage, otkrivanja i progona kaznenih djela" te "zaštite i sprječavanja od prijetnji javnoj sigurnosti", s jedne strane, kao i aktivnosti zemalja članica u odnosu na nacionalnu sigurnost te aktivnosti agencija ili jedinica koje se bave pitanjima nacionalne sigurnosti, s druge strane. Granica između navedena dva područja – prvo nominalno u potpunosti unutar, a drugo formalno u potpunosti izvan EU prava – je poprilično nejasna (oso

161 Presuda Suda od 10. srpnja 1984, Campus Oil Limited i drugi protiv Ministarstva industrije i energije i drugih, Slučaj 72/83, ECR 1984-02727, dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61983CJ0072&from=EN

162 Na primjer: http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (na Nizozemskom)

163 Vijeće Europske unije, Međuinstitucionalni dokument: 2017/0228 (COD), Uvodna izjava (12a), na p. 3, dostupno na: http://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf

164 U Velikoj Britaniji je postojale su prijepori po pitanju progona i osude takvih prosvjednika sukladno antiterorističkom zakonodavstvu – tj. sukladno zakonu o javnoj sigurnosti – a ne prema uobičajenom kaznenom zakonu o prijestupima, vidi: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-showleniency. Slučaj je predmet žalbe.

165 Usput, također rasprava u odjeljku 1.4.6, ispod, o razmjeni osobnih podataka između različitih entiteta uraličitim EU režimima zaštite podataka.

bito u odnosu na vrlo oštro zacrtane kategorije "terorizma", ne u potpunosti jasno razgraničene kategorije poput terorizma, kibernetičkog kriminala, kibernetičke sigurnosti, itd.).[166] Naime:[167]

> U pojedinim državama, agencije postaju hibridi s dvostrukom ulogom borbe protiv kriminala i zaštite nacionalne sigurnosti. Američki savezni istražni ured (FBI) je odličan primjer,[168] međutim u Velikoj Britaniji, GCHQ također usko surađuje s agencijama za provođenje zakona.[169]

Predmetno pitanje neće biti detaljno objašnjeno u ovom dijelu, ali će biti obuhvaćeno u odlomku 1.4.6, u nastavku, o prijenosu osobnih podataka od strane voditelja obrade iz područja obuhvaćenog jednom kategorijom EU zakona o zaštiti osobnih podataka, voditelju obrade koji podliježe drugoj kategoriji EU prava – ili, u slučaju agencija za nacionalnu sigurnost, koje uopće ne podliježe pravu EU.

S druge strane, razlika između obrade osobnih podataka iz nadležnosti LED-a i obrade osobnih podataka od strane EU institucija, tijela, ureda i agencija je jasna te je obuhvaćena novom Uredbom usvojenom 2018. godine, kao što je objašnjeno u odjeljku 1.4.6, u nastavku.

ii. Obuhvaćeni subjekti

U odnosu na pitanje područja primjene, LED definira "nadležna tijela" u čl. 1(1) kao:

(a) svako javno tijelo nadležno za sprječavanje, istragu, otkrivanje ili kazneni progon kaznenih djela ili provedbu kazni za kaznena djela, uključujući zaštitu i sprječavanje prijetnji javnoj sigurnosti; ili

(b) svako tijelo ili subjekt kojem su, zakonom države članice, povjerene javne ovlasti u odnosu na sprječavanje, istragu, otkrivanje ili kazneni progon kaznenih djela ili provedba kazni za kaznena djela, uključujući zaštitu i sprječavanje prijetnji javnoj sigurnosti. (članak 3(7))

Kako je već istaknuto, ovo pitanje moguće je proširiti daleko izvan policije i agencija koje čine "prvu liniju" provedbe zakona, tako da uključuje, ovisno o nacionalnom ustavnom uređenju, lokalna i regionalna javna tijela - agencije za socijalnu skrb, zdravlje i sigurnost, tijela koja nadziru financijske institucije, agencije za zaštitu životinja i okoliša, carinske i porezne agencije te ostale – kada god im se dodijele javne ovlasti u odnosu na kaznena djela ili prijetnje javnoj sigurnosti koje bi mogle uključivati kaznena djela koja se nalaze u njihovoj nadležnosti.

Također kako je već navedeno, obrada osobnih podataka od strane takvih tijela u vezi s aktivnostima koje nisu povezane s kaznenim pitanjima u nadležnosti je GDPR-a, a ne LED-a te isto može biti i u pogledu obrade osobnih podataka od strane nadležnih tijela u vezi s prijetnjama javnoj sigurnosti koja ne uključuju kaznena djela – kao što su oluje, poplave, epidemije ili upravljanje sportskim događajima koji nisu povezani s mogućim kaznenim djelima.

iii. obuhvaćeni načini obrade

S obzirom na sredstva koja se koriste pri obradi, u skladu s ostalim EU instrumentima za zaštitu podataka, LED se odnosi na:

166 Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundries of Law: Exploring Transprency, Accountability, and Oversight of Government Surveillance Regimes, komparativno izvješće koje obuhvaća Kolumbiju, DR Kongo, Egipt, Francusku, Njemačku, Indiju, Keniju, Mijanmar, Pakistan, Rusiju, Južnu Afriku, Tursku, UK, SAD, pripremljeno za World Wide Web Foundation, siječanj 2017, u posebnom odjeljku 2.3.1, dostupno na: https://ssrn.com/abstract=2894490

167 Idem, p. 27. Proširenje uloge policije po pitanju preventivnog djelovanja nije novo.

168 Sadržaj na FBI-evoj web stranici pod naslovom "Suočavanje s prijetnjama cyber sigurnosti države" ističe kako je FBI zadužen kako za zaštitu nacionalne sigurnosti Sjedinjenih Američkih Država, tako i za provođenje zakona općenito, naglašavajući kako su "ove uloge dopunske, ovisno o tome potječu li prijetnje cyber sigurnosti od nacionalnih država, terorističkih organizacija ili transnacionalnih kriminalih organizacija; s ponekad nejasno definiranim međusobnim granicama". Vidi: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity FBI je nedavno izmijenio svoju brošuru kako bi opisao "primarnu funkciju" koja više nije usmjerena na provedbu zakona, već je sada usmjerena na "nacionalnu sigurnost". Vidi The Cable, 5. siječnja 2014., na: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthas h.4DrWhlRV.dpbs Opasnost nejasno postavljenih granica, vidi: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work [original note]

169 Vidi Computer Weekly, "GCHQ and NCA join forces to police dark web", 9. studenog 2015., na: http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web

> obradu osobnih podataka u cijelosti ili djelomično automatiziranim sredstvima te na neautomatiziranu obradu osobnih podataka koji čine dio arhivskog sustava ili su namijenjeni da postanu dijelom arhivskog sustava.

Drugim riječima, LED se primjenjuje na svu obradu osobnih podataka automatiziranim sredstvima kao i na obradu svih osobnih podataka koji se nalaze u strukturiranim priručnim datotekama unutar određenog područja primjene u smislu obuhvaćenih aktivnosti i entiteta.

Važno je istaknuti, za razliku od prethodne Okvirne odluke iz 2008., u odlomku 1.3.6. (iznad), LED se primjenjuje ne samo na osobne podatke koji se razmjenjuju između država članica, već i na nacionalnu obradu osobnih podataka u svrhu provođenja zakona. Kako Komisija ističe, Direktiva bi trebala "olakšati suradnju policije i tijela nadležnih za kazneno pravosuđe diljem EU".[170]

Slobodno kretanje podataka između nadležnih tijela različitih država članica

Iako Direktiva "državama članicama ne sprječava postavljanje viših zaštitnih mjera od onih uspostavljenih samom Direktivom" (čl. 1(3)), država članica koja postavi takve više standarde ne smije zabraniti ili ograničiti slobodnu razmjenu osobnih podataka između država članica, što je i sama svrha Direktive (čl. 1(2)(b)). S druge strane, ako država članica svojim zakonodavstvom predvidi specifične uvjete za određenu obradu (npr. za profiliranje) ili moguće, za obradu određenih vrsta podataka (npr. biometrijskih podataka) – tada država članica ne samo što može, već i mora:

> osigurati da nadležno tijelo koje šalje podatke informira primatelja osobnih podataka o takvim uvjetima i zahtjevu da se ti uvjeti ispoštuju (čl. 9(3)).

Međutim, države članice, sukladno ovoj odredbi, ne mogu postavljati uvjete primateljima u drugim državama članicama koji surađuju u pravosudnim i policijskim pitanjima, osim onih koji su određeni za "slične prijenose" domaćim primateljima te vrste (čl. 9(4)).

(O prijenosu osobnih podataka u nečlanice EU, vidjeti pod tim podnaslovom, ispod).

SADRŽAJ

Mnoge odredbe LED-a vrlo su slične odredbama GDPR-a – ali samo do određene točke, kako bi ukazale na posebno značenje primjene zakona u cilju sprječavanja kriminalnih prijetnji javnoj sigurnosti.

Definicije glavnih pojmova u čl. 3 – "osobni podaci", "obrada", " ograničavanje obrade", " izrada profila", "pseudominizacija", " sustav pohrane", " nadležno tijelo", " voditelj obrade", "izvršitelj obrade", "primatelj", "povreda osobnih podataka", "genetski podaci", "biometrijski podaci", " podaci koji se odnose na zdravlje" – identične su definicijama istih pojmova u GDPR-u.[171]

Osnovna načela, navedena u čl. 4, također su vrlo slična. Ponajprije, načelo **zakonitosti** – koje je nedostajalo u Okvirnoj odluci 2008. – sada je izričito uvršteno u članak 4(a) i razrađeno u čl. 8(1) – s načelom "transparentnosti" (koje je izravno povezano s načelom zakonitosti i pravednosti u GDPR-u) donekle prikazanim u čl. 8(2) ("Zakon države članice koji regulira obradu unutar opsega ove Direktive, određuje barem ciljeve obrade, osobne podatke koji se obrađuju te svrhu obrade") i odredbama o informiranju ispitanika te pravu na pristup njihovim podacima (iako su u posebnom kontekstu LED-a ta prava podložna širim ograničenjima).

170 Europska komisija, Informativni članak – How will the data protection reform help fight international crime? (Kako će reforma zaštite osobnih podataka pomoći u borbi protiv međunarodnog kriminala), 30. travnja 2018., dostupan na: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

171 Začuđujuće, dok postavlja sve prethodno navedene pojmove identično onima u GDPR-u, LED ne definira "treću stranu" – unatoč tome što druga definicija (primatelja) izričito spominje treće strane.

Načelo ograničenja svrhe je ograničeno na način da se osobni podaci prikupljeni od strane bilo kojeg prethodno spomenutog nadležnog tijela u svrhu provođenja zakona ili javne sigurnosti, mogu koristiti **u bilo koju drugu svrhu, sve dok je takva obrada "odobrena od strane (čitaj: bilo kojeg) prava Unije ili zemlje članice"** (čl. 9(1), prva rečenica), uz odredbu iz čl. 9(1), druga rečenica, koja glasi:

Ako se osobni podaci obrađuju u druge svrhe, primjenjuje se Uredba (EU) 2016/679 (GDPR), osim ako se obrada obavlja kao djelatnost koja je izvan područja primjene prava EU. [172]

Iz navedenog proizlazi da svaki podatak za provedbu zakona koji se čini dostupnim kao "autorizacija" zakona, još uvijek mora biti ograničen na ono što je "relevantno" i "nužno" za "zakonitu" svrhu. U načelu, vrlo je važna uloga službenika za zaštitu podataka koji djeluje za pojedince koji otkrivaju podatke i primatelje. Međutim, u nekim zemljama zakon može jednostavno odrediti da se određeni podaci pri provedbi zakona moraju, u posebnim okolnostima (npr. kada se dobije ovlaštenje od visokog dužnosnika) učiniti dostupnim i agencijama nevezanim za provedbu zakona.

Direktiva zahtijeva da država članica postavi ograničenja zadržavanja podataka za obradu podataka sukladno Direktivi (čl. 5) kao i da se postavi jasna granica između osobnih podataka različitih kategorija ispitanika, kao što su osumnjičenici, osuđenici za kaznena djela, žrtve, svjedoci itd. (čl. 6). Također propisuje da "države članice osiguraju mogućnost razlikovanja osobnih podataka temeljenih na činjenicama, od osobnih podataka temeljenih na osobnim procjenama" (čl. 7(1)).

LED također (kao i GDPR) zahtijeva da voditelji obrade usvoje **najnovija sigurnosna rješenja**, uzimajući u obzir kontekst, svrhu obrade itd. (čl. 29(1)), te da moraju provesti **procjenu rizika** u tom smislu, a sve u cilju kako bi utvrdili koja razina sigurnosti je prikladna (čl. 29(2)). Također (ponovo kao i GDPR) zahtijeva fizičku i tehničku sigurnost te uvođenje **obveze povjerljivosti za** osoblje (čl. 23).

Također slično kao i u GDPR-u, **povreda osobnih podataka** mora se prijaviti nadležnom tijelu u roku od 72 sata (u slučaju da se ne prijavi u tom razdoblju, zakašnjenje mora biti opravdano) (čl. 30) te je nužno informirati ispitanike o nastaloj povredi "bez odgode", "gdje je izgledno da će nastala povreda osobnih podataka prouzročiti visok rizik u odnosu na prava i slobode fizičkih osoba" (čl. 31).

Odredbe LED-a vezane uz obradu **osjetljivih podataka** – tj. "podataka koji otkrivaju rasno ili etničko porijeklo, političko opredjeljenje, vjerska uvjerenja ili sindikalno članstvo, genske podatke, biometrijske podatke (kada se koriste u svrhu nedvojbene identifikacije fizičke osobe), zdravstvene podatke ili podatke koji se odnose na seksualni život ili seksualnu orijentaciju osobe" – postavljene su nešto drugačije nego je to određeno GDPR-om (čl. 9),[173] te LED dopušta obradu takvih podataka:

> samo u slučajevima gdje je to izričito potrebno, uz odgovarajuće zaštitne mjere za prava i slobode ispitanika i to samo:
>
> (a) kada je propisano pravom Unije ili zemlje članice;
>
> (b) kako bi se zaštitili vitalni interesi ispitanika ili druge fizičke osobe; ili
>
> (c) kada se obrada odnosi na podatke koje je ispitanik/građanin sam javno objavio (čl. 10 LED-a, dodatno naglašeno)

Posljednja dva uvjeta odgovaraju izuzecima navedenim i u GDPR-u (odnosno, čl. 9(2)(c) i (e)).[174]

Ukoliko se država članica oslanja na drugi uvjet – kada je dopušteno zakonom – mora biti u mogućnosti dokazati kako je obrada podataka neophodna te kako je bilo kakvo ograničenje vezano uz prava ispitanika/građana podložno odgovarajućim zaštitnim mjerama. Nadalje, (drugačije od onoga što je obuhvaćeno Ok

172 Vidjeti također članak 9(2). Navedeno je ponovno obuhvaćeno pododlomkom 1.4.6, ispod.

173 LED, razumljivo, ne sadrži odredbu u skladu s čl. 10, prva rečenica, GDPR-a, kojom se predviđa obrada osobnih podataka vezano uz kaznene presude i djela koja mora biti "pod kontrolom službenog tijela ili ... ovlaštenog zakonom Unije ili zemlje članice koji osigurava odgovarajuće zaštitne mjere za prava i slobode ispitanika": LED i sami nacionalni zakoni osiguravaju navedeno. Slično tome, nepotrebno je ponavljati u LED-u odredbu iz posljednje rečenice čl. 10 GDPR-a kako se "sveobuhvatni registar kaznenih presuda vodi samo pod nadzorom službenih tijela".

174 Osim što se iznimka vezana za obradu radi zaštite vitalnih interesa ispitanika ili druge osobe sukladno članku 9(2)(c) GDPR-a, primjenjuje samo ako je "ispitanik fizički ili pravno spriječen dati pristanak" – što nije obuhvaćeno LED-om.

virnom odlukom 2008.), ispitanici se sada mogu osloniti na Direktivu pri ostvarivanju svojih prava, s tim da Sud EU može utvrđivati je li određeni nacionalni zakon, usvojen u ovom kontekstu, u skladu sa standardom "stroge nužnosti" te obuhvaća li "odgovarajuće mjere zaštite", a Komisija je ovlaštena za poduzimanje određenih radnji ukoliko postoji sumnja da zakon države članice; koji dopušta obradu osjetljivih podataka u svrhu provedbe zakona/javne sigurnosti, ne ispunjava navedene standarde/uvjete.

Direktiva LED također, kao i GDPR, regulira automatizirano donošenje odluka uključujući profiliranje, ali s određenim razlikama. Konkretno, Direktiva propisuje da takva vrsta obrade mora biti "odobrena zakonodavstvom Unije ili države članice" te je podložna "odgovarajućim zaštitnim mjerama/jamstvima" koje moraju obuhvaćati "barem pravo ljudske intervencije od strane voditelja obrade". Međutim, za razliku od GDPR-a, LED ne propisuje da, kada je riječ o takvom obliku "ljudske intervencije", ispitanik može "izraziti svoje stajalište te... osporiti odluku donesenu automatizirano/na temelju profiliranja".

Osobito, LED navodi kako:

> Profiliranje, koje rezultira diskriminacijom fizičkih osoba s obzirom na posebne kategorije osobnih podataka sukladno čl. 10, zabranjeno je sukladno zakonu Unije. (dodatno naglašeno)

Vezano za pitanje "zakonskog ovlaštenja", također je važno uzeti u obzir da se, prilikom izrade zakonskog prijedloga o ovim pitanjima, važno konzultirati s tijelom nadležnim za zaštitu podataka države članice (čl. 28.2).

Službenici za zaštitu podataka u relevantnim tijelima dužni su s osobitom pažnjom razmotriti na koji način bi se mogli istaknuti novi zahtjevi LED-a – ljudske intervencije i obveza nediskriminacije – te učinkovito primijeniti u praksi pod različitim okolnostima.

S obzirom područje primjene, LED omogućava prilično opsežna ograničenja u vezi prava ispitanika na informiranost o obradi, na pristup njegovim ili njezinim podacima, na ispravljanje ili brisanje podataka koji ne udovoljavaju odgovarajućim standardima kvalitete ili su na neki drugi način obrađeni suprotno postavljenim pravilima unutar ovog instrumenta – ali navedena ograničenja moraju biti u okviru onog što je "nužno" i "proporcionalno" u demokratskom društvu (vidjeti čl. 12 - 16 LED-a, posebno čl. 15). Također, LED omogućava da se navedena prava izvršavaju neizravno, putem nadležnog nadzornog tijela (čl. 17). U slučajevima kada su osobni podaci "sadržani u sudskoj odluci, zapisniku ili spisu koji se obrađuju u postupcima kaznenih istraga i postupaka", prava također mogu biti regulirana odgovarajućim nacionalnim zakonodavstvom (čl. 18). U pravilu, policijski zakoni ili zakoni o kaznenom postupku reguliraju pristup osumnjičene, optužene, okrivljene, osuđene osobe određenim dijelovima odgovarajućih spisa, u određenim fazama postupka (u pravilu, dopuštaju ograničen pristup u ranoj fazi te širi pristup kasnije, posebno ako je osoba formalno optužena) – i takve mjere se mogu i zadržati.

Praktični i formalni zahtjevi

U odnosu na mnoga druga pitanja, LED uvodi praktične i formalne zahtjeve slične GDPR-u.

Posebice, vrlo važno je istaknuti kako LED, kao i GDPR, uključuje novo "načelo odgovornosti" (čl. 4(4))[175] te zahtijeva "uzimajući u obzir prirodu, opseg, kontekst te svrhu obrade kao i prijetnje različitih vjerojatnosti i intenziteta pravima i slobodama fizičkih osoba", svi voditelji obrade na koje se Direktiva odnosi moraju:

> ... primijeniti odgovarajuće tehničke i organizacijske mjere kako bi osigurali i bili u mogućnosti dokazati da se obrada provodi u skladu s Direktivom. (članak 19(1), dodatno naglašeno).

175 Detaljno obuhvaćeno Drugim dijelom, odlomak 2.3, ispod.

U članku se dodaje kako bi se "te mjere trebale preispitati i ažurirati po potrebi" te tamo gdje je to "potrebno", moraju uključivati (sastavljati, usvajati) implementaciju "odgovarajućih politika zaštite podataka" od strane voditelja (čl. 19(1), zadnja rečenica i (2)).

Također, kao i GDPR, LED zahtijeva opsežno bilježenje/čuvanje zapisa i logova (čl. 24 i 25), koji predstavljaju važno sredstvo provjere zakonitosti obrade - što predstavlja poseban izazov u području primjene LED-a.

LED utvrđuje jednake zahtjeve kao i GDPR u odnosu na "zajedničke voditelje obrade" (članak 21(1)) te izvršitelje (članak 22).

LED zahtijeva provođenje procjene učinka na zaštitu osobnih podataka (PUZP, članak 27) pod jednakim uvjetima koje predviđa i GDPR, tj.:

> U slučajevima gdje se s obzirom na način obrade, u pravilu upotrebom novih tehnologija te uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade, očekuje da bi moglo posljedično doći do povećanog rizika u odnosu na prava i slobode fizičkih osoba (čl. 27, dodatno naglašeno).

Nadležno nadzorno tijelo (koje može biti nacionalno tijelo za zaštitu osobnih podataka, ali isto tako može biti i zasebno, pod uvjetom da su ispunjeni uvjeti o neovisnosti itd.: vidi ispod) mora također biti uključeno, kada PUZP "ukazuje na to da bi obrada mogla prouzročiti visok stupanj rizika, ukoliko se ne poduzmu mjere koje bi ublažile prijetnju od strane voditelja obrade" ili gdje (bez obzira na takve mjere) "vrsta obrade, u pravilu pri korištenju novih tehnologija, mehanizama ili procedura, uključuje povećan rizik u odnosu na prava i slobode fizičkih osoba" (članak 28(1)(a) i (b)).

Kao sredstvo doprinosa njegovoj učinkovitoj primjeni, posebno u vezi s načelom odgovornosti, LED predviđa imenovanje službenika za zaštitu podataka (SZP) od strane svakog voditelja obrade (čl. 32), pojašnjava položaj službenika za zaštitu podataka (čl. 33) te navodi njegove obveze (čl. 34). Navedeno je također povezano s GDPR-om, koji zahtijeva imenovanje službenika za zaštitu podataka od strane svih tijela u javnom sektoru.[176] Međutim, LED ne propisuje izričito da službenik za zaštitu podataka mora imati mogućnost neovisnog djelovanja.[177]

Službenici za zaštitu podataka u agencijama za provedbu zakona i drugim agencijama ili tijelima na koje se primjenjuje LED imat će glavnu ulogu u vezi sukladnosti njihove organizacije s načelom odgovornosti i kontinuirane revizije mjera poduzetih u svrhu usklađivanja s ovim načelom; izrade "sporazuma" s bilo kojim zajedničkim voditeljem obrade kao i ugovora s izvršiteljima obrade; konzultacija s agencijom za zaštitu podataka te provođenja procjene učinka na zaštitu osobnih podataka (PUZP) sukladno LED-u.[178]

Međunarodni prijenosi podataka nadležnim tijelima u treće zemlje)

Zbog visokog stupnja osjetljivosti konteksta i predmetnih osobnih podataka u ovom području, poglavlje V LED-a predviđa niz uvjeta koji se odnose na prijenos osobnih podataka u neeuropske države (tzv. treće zemlje) ili međunarodne organizacije, slične uvjetima prijenosa predviđenim u GDPR-u, ali uz dodatna pravila o prijenosu u treće zemlje ili međunarodne organizacije od strane zemlje članice EU, podataka koji su zaprimljeni od druge zemlje članice te o daljnjim prijenosima od strane primatelja treće zemlje nekoj drugoj trećoj zemlji ili međunarodnoj organizaciji – uz određene iznimke iz posebnih razloga, kako je objašnjeno niže.

176 Vidi Drugi dio, odjeljak 2.4.2, ispod.
177 Usp. čl. 38(3) GDPR-a koji propisuje da:
"Voditelj i izvršitelj obrade osiguravaju da službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja tih zadaća. Voditelj obrade ili izvršitelj obrade ne smiju ga razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća. Službenik za zaštitu podataka izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade."
178 Usp. detaljno razmatranje zadaća službenika za zaštitu podataka (SZP) sukladno GDPR-u u Trećem dijelu ovog priručnika.

Međutim, potrebno je uzeti u obzir kako posebno u pogledu međunarodnog prijenosa podataka, LED dopušta produženu odgodu pune primjene pravila navedenih niže, iz posebnih razloga, kako je objašnjeno pod naslovom "Odgoda prijenosa" na kraju ovog dijela o LED-u.

Opći preduvjeti za provođenje takvog prijenosa:

Članak 35. LED-a propisuje tri preduvjeta za prijenos u treće zemlje (potrebno je uzeti u obzir da dva preduvjeta mogu biti izuzeta pod određenim okolnostima, kako je istaknuto):

- prijenos mora biti "nužan" za ispunjenje svrhe iz čl. 1(1), tj. u svrhu sprječavanja, istrage, otkrivanja ili kaznenog progona za kaznena djela ili izvršavanje kazni za počinjena kaznena djela, ili očuvanja ili sprječavanja (kaznenopravnih) prijetnji javnoj sigurnosti;
- prijenos mora biti prema tijelu treće zemlje ili međunarodne organizacije nadležnom za prethodno spomenute svrhe (pri čemu je Međunarodna organizacija kriminalističke policije, Interpol, izričito uključena u Uvodnoj izjavi (25)).[179] Kao što "nadležna tijela" u EU nisu ograničena samo na agencije koje provode zakon, tijela u trećim zemljama kojima podaci mogu biti preneseni, također nisu ograničena samo na agencije za provođenje zakona, sve dok su nadležna (također) i u odnosu na određena kaznena pitanja.

  Treba uzeti u obzir kako se *ovaj preduvjet može izuzeti u određenim situacijama*, pod određenim okolnostima, kako je navedeno niže u pododlomku "*Prijenos drugim tijelima*".
- "*kada su osobni podaci preneseni ili učinjeni dostupnima od druge zemlje članice, ta zemlja članica mora dati* ***prethodno odobrenje*** *za prijenos sukladno svom nacionalnom zakonodavstvu*" (predmet izuzeća, kako je spomenuto niže) (članak 35(1)(a)-(c))

Zadnja odredba odnosi se na prijenos iz jedne države članice u treću zemlju ili međunarodnu organizaciju, osobnih podataka prvotno zaprimljenih od druge države članice, tj. za daljnji prijenos takvih podataka potrebno je "prethodno odobrenje" države članice koja je prvotno pružila podatke.

Potrebno je napomenuti kako se *prethodno odobrenje ne zahtijeva ako:*

je prijenos osobnih podataka nužan za sprječavanje neposrednih i ozbiljnih prijetnji javnoj sigurnosti države članice ili treće zemlje kao i temeljnim interesima države članice te prethodno odobrenje nije moguće pribaviti na vrijeme.

U tom slučaju, "*tijelo nadležno za davanje prethodnog odobrenja [čitaj: tijelo od kojeg bi se trebalo zatražiti prethodno odobrenje ukoliko ne postoji nikakva neposredna prijetnja] bi trebalo biti informirano bez odgađanja*" (čl. 35(2), dodatno naglašeno).

Nakon što se ispune ovi odgovarajući preduvjeti, osobni podaci se mogu proslijediti trećoj zemlji ili međunarodnoj organizaciji ako je **jedan od sljedeća tri uvjeta primjenjiv:**

179 Nastavno na navedeno, može se primijetiti kako Interpol nije "međunarodna organizacija" sukladno uobičajenoj definiciji u međunarodnom javnom pravu, tj. organizacija temeljena na ugovoru ili nekom drugom obliku sukladno međunarodnom pravu: vidi članak 2. Nacrta članaka Komisije za međunarodno pravo o odgovornosti međunarodnih organizacija. Suprotno, Interpol je uspostavljen pod vodstvom policijskih vlasti država sudionica. Na ovu temu, vidi pitanje postavljeno Komisiji od strane Charles Tannocka, MEP, 15. listopada 2013., dostupno na: https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN i odgovor Komisije, dostupan na: https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN Međutim, Interpol se još uvijek često definira kao međunarodna organizacija, također djelomično i od strane EU, koja je usvojila Zajedničko stajalište Vijeća o razmjeni podataka o putovnicama s Interpolom i državama članicama/sudionicama Interpola, uz jamstva zaštite podataka: Zajedničko stajalište Vijeća 2005/69/PUP od 24. siječnja 2005. O razmjeni određenih podataka s Interpolom, SL L 27, 29. siječnja 2005, p. 61, dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005E0069 (o zaštiti podataka, vidi čl. 3)
Također vidi Odluku Vijeća 2007/533/PUP od 12. lipnja 2007. O uspostavi, radu i upotrebi druge generacije Schengenskog informacijskog sustava (SIS II), SL L 205, 7. kolovoza 2007, str. 63, koja zabranjuje prijenos ili dostupnost podataka SIS-II trećim zemljama i međunarodnim organizacijama (čl. 54), ali čini iznimku što se tiče razmjene podataka o ukradenim, nepropisno oduzetim, izgubljenim ili nevažećim putovnicama s Interpolom (čl. 55), dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533
Uvodna izjava (25) LED-a predlaže da se na temelju tog instrumenta može razmjenjivati više osobnih podataka s – i kroz – Interpol, sve dok su opći uvjeti za prijenose podataka međunarodnim organizacijama (I trećim zemljama) navedeni u Direktivi (kako je navedeno u tekstu iznad).

- Komisija je izdala **odluku o primjerenosti** u odnosu na primatelja - treću zemlju ili međunarodnu organizaciju (kako je regulirano člankom 36).

  Međutim, potrebno je napomenuti kako Europska komisija još nije donijela takvu odluku o primjerenosti u okviru Direktive te je takva odredba još uvijek neprimjenjiva.

Ili:

- postoje **"odgovarajuće zaštitne mjere"** kako bi se osiguralo da se osobni podaci, nakon prijenosa, i dalje obrađuju sukladno "odgovarajućim" zaštitnim mjerama zaštite podataka.

  Navedeno je u nastavku objašnjeno u članku 37. koji predviđa da odgovarajuće zaštitne mjere moraju biti propisane **pravno obvezujućim dokumentom** (koji može biti sporazum ili pravno obvezujući administrativni sporazum) (čl. 37(1)(a)) ili "*voditelj obrade [mora]* ***procijeniti*** *sve okolnosti transfera osobnih podataka i [zaključiti] da postoje odgovarajuće zaštitne mjere koje se odnose na zaštitu osobnih podataka*" (čl. 37(1)(b)) – ali u potonjem slučaju, **nadzorno tijelo** mora biti informirano o "kategorijama prijenosa" izvršenim u skladu o ovom odredbom. Nadalje, svaki takav prijenos mora biti "*dokumentiran te dokumentacija treba biti dostupna nadzornom tijelu na zahtjev, uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje prima podatke, opravdanost prijenosa te osobni podaci koji su preneseni*" – čl. 37(3).

  Napominjemo kako spomenuti "**pravno obvezujući dokumenti"** obuhvaćaju "*međunarodne sporazume koji uključuju prijenos osobnih podataka u treće zemlje ili međunarodne organizacije koje su zemlje članice sklopile prije 6. svibnja 2016. godine*" kako je to navedeno u članku 61. LED-a. Navedeni sporazumi, kako članak navodi, "*ostaju na snazi dok se ne izmijene, zamijene ili opozovu*" sve dok su "*sukladni pravu Unije koje se primjenjivalo prije tog datuma*". LED ne određuje datum do kojeg bi se navedeni sporazumi, ukoliko nisu sukladni odredbama LED-a, trebali izmijeniti, zamijeniti ili opozvati – ili čak da su države članice dužne preispitati ih u tu svrhu. Ova problematika dalje se objašnjava niže u tekstu, pod naslovom "Odgoda provedbe".

  Također je važno naglasiti kako se alternativne "**odgovarajuće zaštitne mjere"** odnose samo na zaštitu podataka: ne postoji uvjet (kakav je propisan unutar prva dva sljedeće objašnjenja odstupanja) da se izvrši procjena mogućih utjecaja na ostala "temeljna prava i slobode" pojedinca te ukoliko postoje, preteže li javni interes za prijenos;

ili:

- (u nedostatku odluke o primjerenosti sadržane u članku 36. te primjerenih zaštitnih mjera sukladno članku 37.) ako se primjenjuje **odstupanje za određenu situaciju.** Članak 38. omogućuje takvo odstupanje ukoliko je prijenos "**nužan**" u **pet situacija,** od kojih dvije zahtijevaju provođenje "testa ravnoteže" interesa. Drugačijim redoslijedom od onog u članku, iznimne situacije i uvjeti su sljedeći:
- Osobni podaci se mogu prenijeti u treću zemlju bez odluke o primjerenosti i bez odgovarajućih zaštitnih mjera ukoliko je to "**nužno**" za ispunjenje bilo koje svrhe iz članka 1(1), tj. u svrhu **sprječavanja, istrage, otkrivanja ili progona bilo kakvog kaznenog djela ili izvršenja bilo kakvih kaznenih sankcija ili radi zaštite ili sprječavanja bilo kakvih (kaznenopravnih) prijetnji javnoj sigurnosti** (čl. 38(1)(d)) – osim:

  kada nadležno tijelo za prijenos utvrđuje da temeljna prava i slobode ispitanika prevladavaju nad javnim interesom (čl. 38(2)).

- Osobni podaci se mogu prenijeti u treću zemlju bez odluke o primjerenosti i bez odgovarajućih zaštitnih mjera ukoliko je to "**nužno**" za utvrđivanje, provođenje ili obranu pravnih zahtjeva u odnosu na bilo koju prethodno spomenutu svrhu (čl. 38(1)(e) – ponovno osim:

Kada nadležno tijelo za prijenos utvrđuje da temeljna prava i slobode ispitanika prevladavaju nad javnim interesom (čl. 38(2)).

Naglašavamo kako se prethodno navedene dvije situacije odnose na slučajeve koji predstavljaju ozbiljne dileme u odnosu na ljudska prava: s jedne strane, prijenos je "nužan" za glavni javni interes, ali s druge strane, utječe na temeljna prava i slobode ispitanika – možda na najgore moguće načine, kada se primjerice informacije o osumnjičenom, svjedoku ili žrtvi prenose tijelima u državama koje ozbiljno krše ljudska prava; i tada ne postoje "odgovarajuće zaštitne mjere", čak i u odnosu na daljnju obradu osobnih podataka ispitanika. **Jasno, o takvim prijenosima potrebno je konzultirati se sa službenikom za zaštitu podataka nadležnog tijela te će u tom pogledu isti snositi veliki teret savjetodavne uloge.**

- Osobni podaci mogu se prenositi u treću zemlju bez odluke o primjerenosti i bez odgovarajućih zaštitnih mjera ukoliko je to "**nužno**" **za sprječavanje neposredne i ozbiljne prijetnje javnoj sigurnosti zemlje članice ili treće zemlje** (čl. 38(1)(c)) – *u ovom slučaju očito bez obzira na razmatranje temeljnih prava i sloboda ispitanika (osim ako se to može iščitati iz zahtjeva "nužnosti"?)*
- Osobni podaci mogu se prenositi u treću zemlju bez odluke o primjerenosti i bez odgovarajućih zaštitnih mjera ukoliko je to **"nužno" radi zaštite ključnih interesa ispitanika ili drugih osoba** (čl. 38(1)(a)).
- Osobni podaci mogu se prenositi u treću zemlju bez odluke o primjerenosti i bez odgovarajućih zaštitnih mjera ukoliko je to **"nužno" za zaštitu legitimnih interesa ispitanika,** a isto je propisano zakonom države članice u odnosu na prijenos osobnih podataka (čl. 38(1)(b)).

Podaci preneseni na temelju bilo kojeg od prethodnih pet izuzetaka moraju biti **"strogo nužni"** (Uvodna izjava (72)) i **dokumentirani** te:

dokumentacija **treba biti dostupna nadzornom tijelu na njegov zahtjev,** uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje zaprima podatke te o opravdanosti prijenosa i osobnim podacima koji su preneseni (čl. 38(3), dodatno naglašeno).

Svrha predmetne dokumentacije i njezine dostupnosti nadležnom tijelu je u tome da nadležno tijelo (naknadno) "*nadzire zakonitost prijenosa*" (Uvodna izjava (72)). Uvodna izjava (72) dodaje sljedeće:

[Prethodno navedene izuzetke/odstupanja] treba **tumačiti restriktivno** te se **ne bi smjeli dopustiti česti, masovni i strukturni** prijenosi osobnih podataka ili prijenosi podataka velikih razmjera, već ih je potrebno ograničiti na podatke koji su nužni

Ponovno, svaki službenik za zaštitu podataka u određenoj organizaciji snosio bi glavnu odgovornost u odnosu na dokumentaciju te u odnosu na komunikaciju o relevantnim problemima s nadležnim tijelom. [180]

PRIJENOS DRUGIM TIJELIMA U TREĆIM ZEMLJAMA

Kako je prethodno naglašeno, u principu se sve gore navedene vrste prijenosa mogu izvršiti prema tijelima u odgovarajućoj trećoj zemlji, koja imaju ovlasti u odnosu na svrhe navedene u članku 1(1) Direktive, tj. u vezi sa "*sprječavanjem, istragom, otkrivanjem ili progonom kaznenih djela ili izvršenjem kazni za kaznena djela, uključujući zaštitu i sprječavanje [kaznenopravnih] prijetnji javnoj sigurnosti*" (čl. 35(1)(b)) (iako primatelji ne moraju biti agencije za provođenje zakona; oni mogu uključivati druga javna tijela u čijoj su nadležnosti neke od zadaća i ovlasti u odnosu na kriminal ili javnu sigurnost).

Međutim, članak 39. LED-a dopušta **odstupanja** od ovog pravila, pod naslovom "*Prijenos osobnih podataka primateljima sa sjedištem u trećim zemljama*" (pod tim se podrazumijevaju i drugi primatelji osim tijela koja su, u određenoj trećoj zemlji, nadležna za pitanja navedena u članku 1(1) Direktive).

180 Vidi Treći dio ovog Priručnika, *Zadaće službenika za zaštitu podataka,* Zadaće 1 – 5 i 12.

Uvodna izjava (73) objašnjava razloge za navedena odstupanja (za navedene izuzetke) (prijelomi odlomaka i dodani naglasci):

> Nadležna tijela država članica primjenjuju bilateralne ili multilateralne međunarodne sporazume, sklopljene s trećim zemljama u području pravosudne suradnje u vezi kaznenih pitanja te policijske suradnje u svrhu razmjene bitnih informacija potrebnih za obavljanje zadaća koje im nalaže zakon. U načelu, to se odvija u slučaju suradnje tijela trećih zemalja, nadležnih za ispunjenje svrhe sukladno ovoj Direktivi, ponekad i uz odsustvo bilateralnih ili multilateralnih međunarodnih sporazuma.
>
> **Međutim, u posebnim pojedinačnim slučajevima, redoviti postupci koji zahtijevaju kontaktiranje takvog u trećoj zemlji mogu biti neučinkoviti ili neprikladni, posebno ukoliko se prijenos ne može izvršiti na vrijeme ili ukoliko tijelo [čitaj: nadležna agencija za provođenje zakona] u trećoj zemlji ne poštuje vladavinu prava ili međunarodne norme i standarde koji se odnose na ljudska prava te zbog toga nadležno tijelo države članice ne može donijeti odluku o prijenosu osobnih podataka izravno primateljima [čitaj: drugi, nevladina tijela] čiji je poslovni nastan na području trećih zemalja.**
>
> Ovo bi mogao biti slučaj kada je hitno potrebno izvršiti prijenos osobnih podataka u svrhu spašavanja života osobe koja se nalazi u opasnosti da postane žrtva kaznenog djela ili u svrhu sprječavanja neposrednog počinjenja kaznenog djela, uključujući terorizam.
>
> Iako bi se takav prijenos između nadležnih tijela i primatelja, sa sjedištem u trećim zemljama, trebao provoditi samo u posebnim slučajevima, ova Direktiva trebala bi sadržavati odredbe za reguliranje takvih slučajeva.
>
> Takve odredbe se ne smiju smatrati odstupanjima/izuzecima od postojećih bilateralnih ili multilateralnih međunarodnih sporazuma u području pravosudne suradnje koja se odnosi na kaznena pitanja ili policijske suradnje. Navedene odredbe bi se trebale primjenjivati zajedno s ostalim odredbama sadržanim u ovoj Direktivi, posebno one koje se odnose na zakonitost obrade i Poglavlje V.

Članak 39(1) se može parafrazirati na sljedeći način:[181]

> Zakon Unije ili države članice može predvidjeti da tijela za provedbu zakona, u individualnim ili posebnim slučajevima, izravno prenose osobne podatke primateljima koji imaju sjedište u trećim zemljama, a koji nisu nadležni u odnosu na kaznena i pitanja javne sigurnosti, ali samo ukoliko je to sukladno drugim odredbama ove Direktive i ako su ispunjeni svi navedeni uvjeti:...

LED ne definira precizno obilježja odgovarajućih "drugih tijela". S obzirom da se članak **39. primjenjuje na situacije koje su u prvom redu osjetljive na pitanja ljudskih prava** (vidi naglašenu rečenicu citata Uvodne izjave (73), iznad), pretpostavlja se da su predviđeni primatelji u trećoj zemlji, oni u koje tijelo koje obavlja prijenos iz određene zemlje članice ima **posebno povjerenje.** Konkretno, tijelo koje obavlja prijenos mora pouzdano znati da primatelj kao tijelo koje ne provodi zakon neće proslijediti informacije tijelima za provedbu zakona treće zemlje koja "*ne poštuje zakonska pravila međunarodnih normi i standarda koji se odnose na ljudska prava*". Odgovarajuća procjena od slučaja do slučaja će uvijek biti posebno osjetljiva te bi se trebala **vrlo pažljivo dokumentirati** (uključujući razloge pretpostavljanja da podaci mogu biti preneseni agenciji od povjerenja, bez straha da će isti završiti u rukama manje savjesnih tijela u trećoj zemlji).

Za prijenose koji nisu obuhvaćeni međunarodnim sporazumima (kako se posebno raspravlja u nastavku),

181 Tekst članka 39(1) glasi:
"Odstupajući od članka 35. stavka 1. točke (b) i ne dovodeći u pitanje nijedan međunarodni sporazum iz stavka 2. ovog članka, pravom Unije ili pravom države članice može se osigurati da nadležna tijela iz članka 3. točke 7. podtočke (a) mogu, u pojedinačnim i posebnim slučajevima, prenijeti osobne podatke izravno primateljima s poslovnim nastanom u trećim zemljama samo ako se poštuju druge odredbe ove Direktive i ako su ispunjeni svi sljedeći uvjeti:."

članak 39(1) postavlja **pet kumulativnih uvjeta** za odgovarajuće prijenose. Podaci mogu biti preneseni odgovarajućim nevladinim primateljima u trećoj zemlji ukoliko (uz dodatak pojašnjenja u uglatim zagradama i napomena uz klauzule):

a. prijenos je **strogo nužan** za izvršavanje zadaće nadležnog tijela [u odgovarajućoj državi članici EU] kako je predviđeno zakonom Unije ili države članice, za potrebe ispunjenja svrha navedenih u članku 1(1) [tj. **u odnosu na kaznena pitanja ili pitanja javne sigurnosti EU ili države članice**].

b. nadležno tijelo za prijenos utvrđuje kako **ne postoje temeljna prava i slobode ispitanika koji pretežu u odnosu na javni interes** koji zahtijeva prijenos u predmetnom slučaju.

   Imati na umu kako navedeno određenje nije ograničeno na interese zaštite podataka ispitanika, već je potrebno sagledati općenito je li određena treća zemlja i agencija u toj zemlji "*poštovala odredbe zakona koje se odnose na međunarodne norme i standarde ljudskih prava*". Određenje bi trebalo biti temeljeno **na svakom slučaju posebno.**

c. nadležno tijelo za prijenos smatra kako je **prijenos tijelu nadležnom za ispunjenje svrha navedenih u** članku **1(1)** [kaznena i pitanja javne sigurnosti] u trećoj zemlji **neučinkovit ili neprimjeren,** posebno iz razloga što *se prijenos ne može izvršiti u primjerenom roku* – ili, treba dodati, jer bi to bilo "neprimjereno" iz drugih razloga: vidi bilješku pod sljedećom klauzulom.

d. **je tijelo nadležno za svrhe iz** članka **1(1) u trećoj zemlji *obavješteno*** bez nepotrebne odgode, osim ukoliko je to **neučinkovito i neprimjereno.**

   Potrebno je naglasiti kako bi se prenošenje tijelu za provedbu zakona, koje je inače najrelevantnije i najprikladnije, može tumačiti kao **"neprimjereno"** u odnosu na situaciju u kojoj agencija "*[ne] poštuje odredbe zakona koje se odnose na međunarodne norme i standarde ljudskih prava*". Upućivanje na **"neučinkovitost"** te agencije može se odnositi na to da je *inače neučinkovita, spora, nekompetentna ili možda korumpirana.*

e. **tijelo nadležno za prijenos informira primatelja o posebnoj svrsi ili svrhama obrade osobnih podataka koje *predviđaju da je takva obrada nužna.***

   Naglasak je na tome kako se pod tim podrazumijeva da tijelo primatelj u trećoj zemlji mora pružiti (snažna i obvezujuća) **jamstva** da će se pridržavati ovih odredbi te da će koristiti podatke zaprimljene od EU tijela za provođenje zakona samo za određene, predviđene svrhe i tada će upotrijebiti te podatke (isključivo) u onoj mjeri u kojoj je to nužno za izvršenje predviđenih svrha.

Osim ispunjenja navedenih posebnih svrha, kako je navedeno, članak 39(1) naglašava kako se "*[sve] ostale odredbe ove Direktive*" također moraju poštivati (vidi također zadnju rečenicu Uvodne izjave (73), navedenu iznad, koja ističe kako to uključuje "posebno one [odredbe] o zakonitosti obrade i Poglavlje V", tj. ostale odredbe o prijenosu podataka).

Sve navedeno, međutim, "**ne dovodi u pitanje bilo koji međunarodni sporazum**" (čl. 39(1)), pod kojim se podrazumijeva:

> svaki bilateralni ili multilateralni međunarodni sporazum sklopljen između država članica i trećih zemalja u području pravosudne suradnje u kaznenim pitanjima i policijske suradnje (čl. 39(2)).

Navedeno bi trebalo čitati zajedno s člankom 61., koji se odnosi na LED-ovu "*Vezu s prethodno sklopljenim međunarodnim ugovorima u području pravosudne suradnje u kaznenim pitanjima i policijske suradnje*" koji ističe kako:

> međunarodni sporazumi koji uključuju prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, a koje su države članice sklopile prije 6. svibnja 2016. i koji su sukladni zakonu Unije, primjenjivi prije tog datuma, ostaju na snazi do trenutka izmjene, zamjene ili opoziva.

LED ne određuje datum do kojeg bi navedeni sporazumi, ukoliko nisu u skladu s odredbama LED-a, trebali biti izmijenjeni, zamijenjeni ili opozvani – ili obvezu država članica da preispitaju predmetne ugovore u svrhu njihova usklađivanja s Direktivom.[182] Međutim, članak 62. određuje da:

> do 6. svibnja 2022. te sljedeće svake četiri godine, Komisija Europskom parlamentu i Vijeću podnosi **izvješće o ocjeni i pregledu ove Direktive.** Izvješća moraju biti javno dostupna (dodatno naglašeno).

Ta izvješća uključuju "*posebno, primjenu i funkcioniranje Poglavlja V u odnosu na prijenos osobnih podataka u treće zemlje ili međunarodne organizacije*" (čl. 62(2)), s "posebnim naglaskom" na odluku o primjerenosti iz članka 36(3) kao i **prijenos "drugim tijelima" iz** članka **39,** kako je objašnjeno. Komisija može, osim toga, u tom kontekstu, "*zahtijevati informaciju od zemalja članica te nadležnih tijela*" (čl. 62(3)) uključujući, pretpostavlja se, jedan od prethodno spomenutih međunarodnih sporazuma koje su sklopili. Također, Komisija može, na osnovi prvog izvješća, **predložiti** uvođenje **promjena** u predmetne ugovore ili **sugerirati** na koji način se isti trebaju uskladiti s odredbama LED-a – međutim ovo nije određeno Direktivom (za razliku od akata Unije iz ovog područja).[183]

Prema Komisiji, LED će dovesti do "**snažnije međunarodne suradnje**":[184]

> Suradnja između EU policijskih i pravosudnih tijela sa zemljama nečlanicama će također ojačati [uz LED] jer će postojati jasnija pravila za međunarodne prijenose podataka u odnosu na kaznena djela. Nova pravila osigurat će da se prijenosi odvijaju uz odgovarajuću razinu zaštite podataka.

Međutim, kako je objašnjeno pod naslovom "*Nepravodobno prenošenje*", bit će potreban protok određenog vremena prije nego spomenuta pravila u potpunosti budu primjenjiva.

Nadzor i provođenje

Poglavlje VI LED-a zahtijeva uspostavu **neovisnih nadzornih tijela** u državama članicama, zaduženih za nadzor i provođenje odredaba nacionalnih zakona usvojenih u svrhu implementacije ("prenošenja") Direktive te drugih povezanih zadaća (vidi članak 41 – 46 LED-a). Nadležno nadzorno tijelo ili tijela mogu biti, ali ne nužno, opća nadzorna tijela uspostavljena GDPR-om (čl. 41(3)): u nekim zemljama postoje posebna nadzorna tijela koja nadziru obradu osobnih podataka od strane policije i državnih agencija, dok u drugim opće nadzorno tijelo (TZP) također ima istu zadaću. Međutim, u nekim zemljama (posebno u federalnim), postoje razlike između nacionalnih (federalnih) i lokalnih ili regionalnih tijela.

Kao i općim TZP-ovima uspostavljenim temeljem GDPR-a, nadzornim tijelima nadležnim u odnosu na pitanja iz opsega LED-a nužno je dodijeliti **opsežne ovlasti,** uključujući pravo da zahtijevaju (i dobiju) "***pristup svim osobnim podacima*** *koji se obrađuju te* ***svim informacijama*** *potrebnim za ispunjenje ove zadaće***"**; ovlast izdavanja ***upozorenja*** voditelju ili izvršitelju obrade kojim bi se **naložilo** voditelju ili izvršitelju obrade **usklađenje** poslovanja s Direktivom, "*gdje je to prikladno, na određeni način i u određenom roku, posebno nalaganjem ispravljanja ili brisanja osobnih podataka ili zabranom obrade*" te izricanje ***privremenog ili trajnog ograničenja, uključujući zabranu*** obrade; ovlast ***pokretanja pravnih postupaka*** protiv voditelja ili izvršitelja koji postupaju protivno Direktivi ili upućivanje takvih pitanja na znanje nadležnom (državnoodvjetničkom) tijelu (čl. 47(1), (2) i (5) LED). Nadležna tijela također imaju važnu **savjetodavnu ulogu** te moraju imati ovlaštenje:

---

182 Također, nismo svjesni nikakve revizije učinjene prije uvođenja LED-a, sukladno kojoj su međunarodni ugovori koji uključuju prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, a koji su sklopljeni sa zemljama članicama, prethodno usklađeni sa zakonom Unije.

183 Članak 62(6) propisuje da do 6. svibnja 2019. Komisija treba pregledati "*druge pravne akte usvojene od strane Unije, koji uređuju obradu od strane nadležnih tijela u svrhe propisane člankom 1(1), uključujući one koji su u skladu s* članka*m 60, a sve u svrhu procjene potrebe usklađenja s Direktivom te po potrebi izložiti prijedloge izmjene tih akata kako bi se osigurao dosljedan pristup zaštiti osobnih podataka u opsegu ove Direktive*". Vidi u nastavku naslov "*Nepravodobno prenošenje*".

184 Europska komisija, Informativni članak – Kako će reforma zaštite podataka pomoći u borbi protiv međunarodnog kriminala? (bilješka 176, iznad)

da na [vlastitu] inicijativu ili zahtjev, izdaju **mišljenja [svom] nacionalnom parlamentu i … vladi** ili, sukladno nacionalnom zakonu, drugim institucijama i tijelima kao i javnosti o različitim pitanjima zaštite osobnih podataka (čl. 47(3), dodatno naglašeno).

Također su dužna objavljivati **godišnja izvješća** o svojim aktivnostima, "*koja mogu sadržavati popis vrsta prijavljenih kršenja pravila te vrste izrečenih kazni.*" (čl. 49).

Odluke nadležnih tijela moraju, međutim, podlijegati "*odgovarajućim zaštitnim mjerama, uključujući učinkovitim pravnim sredstvima i propisanim postupanjimaa, sukladno zakonu Unije i države članice u odnosu na Poglavlje*" (čl. 47(4)).

Značajno, LED propisuje da:

Države članice osiguravaju nadležnim tijelima učinkovite mehanizme za poticanje povjerljivog prijavljivanja povreda sukladno ovoj Direktivi (čl. 48).

Ova odredba je u skladu s nedavno usvojenom Direktivom o zaštiti osoba koje prijavljuju nepravilnosti (*Whistleblowing Directive)*.[185]

Članak 50. predviđa **međusobnu pomoć** između nadzornih tijela država članica EU, nadležnih u odnosu na obradu osobnih podataka koja je regulirana LED-om. Nadalje, **Europski odbor za zaštitu podataka,** osnovan u okviru GDPR-a, također ima ovlasti u odnosu na obradu iz područja primjene LED-a (čl. 51). To uključuje izdavanje **smjernica, preporuka i najboljih praksi** u vezi pitanja iz nadležnosti Direktive te izdavanje:

mišljenja za procjenu primjerenosti razine zaštite u trećoj zemlji, teritoriju jedne ili više zasebnih sektora u trećoj zemlji ili međunarodnoj organizaciji, uključujući procjenu osigurava li takva treća zemlja, teritorij, zaseban sektor ili međunarodna organizacija primjerenu razinu zaštite (čl. 51(1)(g)).

Odbor mora proslijediti mišljenja, smjernice, preporuke i najbolje prakse Komisiji (i Odboru osnovanom člankom 93 GDPR-a) te ih mora učiniti javno dostupnim (čl. 51(3)); a Komisija mora povratno informirati Odbor o aktivnostima koje je poduzela kao odgovor (čl. 51(4)).

Pravni lijekovi, odgovornost i kazne

Poglavlje VIII sadrži pravne lijekove, odgovornost i kazne koji se moraju prenijeti u nacionalne zakone sukladno LED-u.

Ukratko, u skladu s GDPR-om, svakom ispitaniku mora biti zajamčeno **pravo podnošenja pritužbe** nadležnom nadzornom tijelu, ukoliko ispitanik smatra da je obrada njegovih osobnih podataka suprotna odredbama sadržanim u Direktivi (čl. 52), kao i pravo ulaganja **djelotvornog pravnog lijeka** protiv bilo koje obvezujuće odluke nadležnog nadzornog tijela koja se odnosi na nju ili njega (čl. 53) te protiv voditelja ili izvršitelja obrade koji su u nadležnosti (sukladno nacionalnom zakonu) LED-a, "*ukoliko smatra da su njegova ili njezina prava, zajamčena odredbama usvojenim ovom Direktivom, povrijeđena kao rezultat obrade njegovih ili njezinih osobnih podataka suprotno predmetnim odredbama*" (čl. 54). Štoviše (ponovno u skladu s GDPR-om):

ispitanik ima pravo **ovlastiti neprofitno tijelo, organizaciju ili udruženje** koje je pravilno osnovano

185 Direktiva Europskog parlamenta i Vijeća o zaštiti osoba koje prijavljuju kršenje prava Unije, 2019. U vrijeme pripremanja ovog priručnika, tekst još uvijek nije objavljen u Službenom listu (te još nema broj), međutim isti je usvojen od strane Europskog parlamenta 16. travnja 2019. (što predstavlja konačnu verziju, podložnu jezičnom uređivanju i prevođenju) dostupan putem poveznice: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_EN.html?redirect

> skladu s pravom države članice, u čijem se statutu navode ciljevi od javnog interesa te koje je aktivno na području zaštite prava i sloboda ispitanika s obzirom na zaštitu njegovih osobnih podataka, **da podnese pritužbu u njegovo ime i da ostvari prava iz** članaka **52., 53. i 54. u njegovo ime** (članak 55., dodatno naglašeno).

Ispitanik također ima **pravo na naknadu štete** za materijalna i nematerijalnu štetu koja je nastala zbog obrade suprotne LED-u (čl. 56).

Konačno, države članice moraju predvidjeti "**učinkovite, proporcionalne i odvraćajuće kazne"** za svako kršenje LED-a.

Odgođeni prijenos

Kako je već spomenuto u ranijim pododlomcima, svaka obrada osobnih podataka u svrhu provođenja zakona i javne sigurnosti ne mora biti u skladu s LED-om ili nacionalnim zakonima kojima se LED prenosi na nacionalnu razinu: Direktiva sadrži niz odredbi koje omogućavaju određene instrumente i aktivnosti koje će dovesti do usklađenja s Direktivom u nekom budućem vremenu (ili u nekoj nedefiniranoj budućnosti). Odredbe koje omogućavaju odgođenu provedbu odnose se na EU "pravne akte"; ugovore između zemalja članica EU i trećih zemalja ili međunarodnih organizacija (uključujući Interpol), kao i posebne automatizirane sustave obrade zemalja članica u kaznenopravnom području i području javne sigurnosti.

Odgođena provedba u odnosu na EU pravne akte:

Članak 60. LED-a propisuje približno 123 EU instrumenta ("pravnih akata" različitih vrsta) koji se odnose na pitanja pravosuđa i unutarnjih poslova (PUP)[186] da:

> posebne odredbe o zaštiti osobnih podataka u **pravnim aktima Unije koji su stupili na snagu prije 6. svibnja 2016.** u području pravosudne suradnje i kaznenih pitanja te policijske suradnje, a kojima se uređuje obrada između država članica te pristup imenovanih tijela država članica informacijskom sustavu uspostavljenom u skladu s ugovorima iz opsega Direktive, **ostaju neizmijenjene** (dodatno naglašeno).

Međutim, članak 62(6) LED dalje predviđa da, **do 6. svibnja 2019.,** Komisija ima obvezu **izvršiti reviziju:**

> [svih] drugih pravnih akata [tj. osim LED] usvojenih od strane Unije kojima se uređuje obrada od strane nadležnih tijela u svrhe navedene u članku 1(1) uključujući one navedene u članku 60., **a sve kako bi se procijenilo postoji li potreba njihovog usklađenja s ovom Direktivom te kako bi se, gdje je to primjereno, izradili potrebni prijedlozi za izmjenu tih akata** u svrhu osiguranja dosljednog pristupa zaštiti osobnih podataka u skladu s opsegom Direktive (dodatno naglašeno).

Iz prethodnog proizlazi da ta **približno 123 "druga pravna akta" ne trebaju biti usklađena s LED-om do 6. svibnja 2019.:** jedino što se zahtijeva je njihova **revizija** kako bi se **predložile** izmjene gdje je to potrebno. **Nije određen datum do kojeg je potrebno donijeti stvarne izmjene** ili čak za donošenje odgovarajućih, detaljnih prijedloga za svaki instrument.[187]

U međuvremenu, kako propisuje članak 60., pravila o zaštiti podataka sadržana u približno 123 pravna akta ostaju na snazi i mogu se primjenjivati kao temelj za prijenos osobnih podataka u području kaznenog prava i javne sigurnosti, usprkos tome što možda nisu u skladu s LED-om – pod uvjetom da su ispunjena **tri predu-**

186 Vidi Emilio De Capitani, navedeno djelo (bilješka 141, iznad)
187 U vrijeme pisanja završne verzije prvog izdanja ovog priručnika, početkom svibnja 2019., Komisija još nije iznijela takve prijedloge.

vjeta takvog prijenosa, utvrđena LED-om: da je prijenos (prema mišljenju tijela EU koji vrši isti) "nužan" za ostvarenje svrhe u području kaznenog prava i javne sigurnosti; da je prijenos izvršen prema tijelu u trećoj zemlji nadležnom za ovo područje (osim ukoliko je to tijelo neučinkovito, presporo ili još gore: krši ljudska prava); ukoliko su preneseni podaci izvorno dobiveni od države članice te je ta država članica odobrila prijenos (ili u hitnim situacijama, da je barem bila obavještena o istom); i pod uvjetom da **bilo koji** pravni instrument sadrži "odgovarajuće" mjere zaštite podataka **ili** (ako instrument ne sadrži takve mjere) "*nadležno tijelo EU za prijenos utvrdi da temeljna prava i slobode ispitanika*" ne "*pretežu u odnosu na javni interes u predmetnom prijenosu*".

Ključno je da, prema novom načelu "**odgovornosti**", **sačinjene procjene –** tj. sadrži li odgovarajući pravni instrument "odgovarajuće" mjere zaštite podataka ili o tome preteže li i zašto javni interes prilikom prijenosa potrebu zaštite temeljnih prava i sloboda ispitanika – moraju **biti zabilježene** te po zahtjevu, dane na uvid Europskom odboru za zaštitu podataka (i Sudu).

Svaki službenik za zaštitu podataka (SZP) unutar nadležnog tijela EU mora imati glavnu ulogu u navedenom: prvenstveno, upozoravajući organizaciju na potrebu provođenja testova, a nakon toga i internom provjerom primjenjuju li se ti testovi pravilno te savjetujući se s Europskim nadzornikom za zaštitu podataka u slučaju internih neslaganja ili u vezi određenih pitanja te tematike.

Odgođena provedba u odnosu na ugovore između zemalja članica EU i trećih zemalja i međunarodnih organizacija:

Kako je prethodno navedeno, članak 61. propisuje da:

> međunarodni sporazumi koji uključuju prijenos osobnih podataka u treće zemlje ili međunarodne organizacije, zaključeni od strane država članica prije 6. svibnja 2016. i koji su u skladu s pravom Unije, primjenjivi prije navedenog datuma ostaju na snazi do izmjene, zamjene ili opoziva.

Prijenosi sukladni ugovorima sklopljenim prije svibnja 2016. između država članica i trećih zemalja/ međunarodnih organizacija, mogu se nastaviti, pod uvjetom da su ispunjena tri preduvjeta propisana LED-om: da je prijenos (prema mišljenju tijela EU koji vrši isti) "nužan" za ostvarenje svrhe u području kaznenog prava i javne sigurnosti; da je prijenos izvršen prema tijelu u trećoj zemlji nadležnom za ovo područje (osim ukoliko je to tijelo neučinkovito, presporo ili još gore: krši ljudska prava); ukoliko su preneseni podaci izvorno dobiveni od države članice te je ta država članica odobrila prijenos (ili u hitnim situacijama, da je barem bila obavještena o istom); i pod uvjetom da **bilo koji** pravni instrument sadrži "odgovarajuće" mjere zaštite podataka **ili** (ako instrument ne sadrži takve mjere) "*nadležno tijelo EU za prijenos utvrdi da temeljna prava i slobode ispitanika*" ne "*pretežu u odnosu na javni interes u predmetnom prijenosu*".

Međutim ponovno, prema načelu "**odgovornosti**" procjene tijela – tj. sadrži li ugovor "odgovarajuće" mjere zaštite podataka te ispunjava li zaista zakon Unije prije svibnja 2016 ili prevladava li javni interes za prijenos podataka nad zaštitom temeljnih prava i sloboda ispitanika – moraju biti **zabilježene** te se, na zahtjev, moraju dostaviti nadležnom tijelu (i sudovima).

Također ponovno, svaki službenik za zaštitu podataka (SZP) u odgovarajućem nadležnom tijelu države članice ima glavnu ulogu u navedenom.

Odgođena provedba u odnosu na poseban automatiziran sustav obrade država članica u kaznenopravnom i području javne sigurnosti

Članak 63., koji se posebno bavi prenošenjem odredbi LED-a u nacionalni zakon, u svom prvom paragrafu propisuje sljedeće:[188]

> Države članice će usvojiti i objaviti, do 6. svibnja 2018. zakone, propise i administrativne odredbe nužne za usklađivanje s Direktivom. Iste će bez odlaganja Komisiji dostaviti tekst takvih odredbi. Predmetne odredbe primjenjivat će od 6. svibnja 2018. (dodatno naglašeno)

U načelu, iz navedenog proizlazi da "zakoni, propisi i administrativne odredbe" do tog datuma moraju biti u potpunosti usklađeni s LED-om.

Međutim, članak predviđa određenu **iznimku** u sljedećem članku, u skladu s uvjetima:

> Odstupajući od stavka 1., država članica može predvidjeti da se, **iznimno, ako to zahtijeva nerazmjeran napor**, automatizirani sustavi obrade uspostavljeni prije **6. svibnja 2016**. moraju uskladiti s člankom 25(1) do 6. svibnja 2023.

Treći stavak dopušta još duža odstupanja, uz daljnje uvjete:

Odstupajući od stavaka 1. i 2 ovog članka, država članica može, **u iznimnim okolnostima**, automatizirani sustav obrade kako je navedeno u stavku 2. ovog članka uskladiti s člankom 25(1) **unutar određenog roka nakon roka** iz stavka 2. ovog članka, **ako bi to u suprotnom uzrokovalo ozbiljne poteškoće u radu tog automatiziranog sustava obrade**. Država članica **obavješćuje Komisiju** o razlozima tih ozbiljnih poteškoća te razlozima određenog roka unutar kojeg se taj konkretni automatizirani sustav obrade usklađuje s člankom 25(1). Određeni rok u svakom slučaju ne smije biti kasnije od **6. svibnja 2026**. (dodatno naglašeno). Sve prethodno navedeno ne znači da će potpuna primjena svih zahtjeva LED-a, posebno uključujući one koji se odnose na prijenos podataka u treće zemlje i međunarodne organizacije, potrajati.

Međutim, u međuvremenu je važno podsjetiti da su sukladno Direktivi (suprotno od prethodne Okvirne odluke Vijeća) usklađenost pravila i postupaka Unije i država članica u odnosu na kaznena i pitanja javne sigurnosti sada opravdana. Navedeno u konačnici uključuje i provjeru usklađenosti svih pravila i postupaka s LED-om, uključujući prethodno navedeni test (o tome sadrži li ugovor "odgovarajuće" mjere zaštite podataka ili ispunjava li zakon Unije od prije svibnja 2016; pretežu li javni interes pri prijenosu u odnosu na zaštitu temeljnih prava i sloboda ispitanika; te, u odnosu na bilo kakva kašnjenja usklađivanja s Direktivom, jesu li ispunjeni uvjeti za takva odgađanja navedena u prethodnim stavcima.

1.4.4. Novi instrumenti zaštite podataka u području zajedničke vanjske i sigurnosne politike (ZVSP)

Kao što objašnjava Komisija:[189]

> Lisabonski ugovor 2009. značajno je doprinio jačanju aktivnosti Unije u području vanjskih aktivnosti. Prvenstveno je uspostavljeno mjesto **Visokog predstavnika (High Representative) Unije za vanjske poslove i sigurnosnu politiku.**

188 Posljednji, četvrti, stavak propisuje da: *"države članice Komisiji šalju tekst glavnih odredaba nacionalnog prava koje donesu u području na koje se odnosi ova Direktiva"*. Konkretnija odredba iz prvog stavka naglašava kako je potpuna primjena LED-a zapravo više proces koji će napredovati kroz nekoliko godina, nego jednokratan prijenos.

189 Vidi: https://ec.europa.eu/fpi/about-fpi_en

Također, Ugovorom je uspostavljena i **Europska služba za vanjsko djelovanje (ESVD).** Djeluje od 2011., a predstavlja novu diplomatsku službu EU, koja pomaže Visokom predstavniku u vođenju vanjske politike EU. ESVD upravlja mrežom sastavljenom od **141 EU Delegacije** diljem svijeta.

ESVD djeluje s ciljem osiguravanja konzistentnosti i koordinacije vanjskog djelovanja Unije, na način da priprema prijedloge politika te ih primjenjuje nakon što iste odobri Europsko Vijeće .

Uz ESVD, uspostavljena je i nova služba Komisije, **Služba za instrumente vanjske politike (FPI)** koja snosi odgovornost u pogledu operativnih troškova.

Danas, pod nadzorom [Visokog predstavnika] te usko surađujući s ESVD-om i EU delegacijama, FPI je zadužen za ... provedbu proračuna Zajedničke vanjske i sigurnosne politike (ZVSP) [kao i raznih drugih instrumenata i aktivnosti]...[190]

Proračun koji obuhvaća širok spektar aktivnosti FPI-a 2014. godine iznosio je 733 milijuna.

Posao koji obavljaju HR, ESVD i osoblje FPI službe često obuhvaća obradu osobnih podataka, npr. u odnosu na izricanje sankcija pojedincima ili zamrzavanja njihove imovine.[191]

Međutim, takva obrada nije predmet istih pravila EU ugovora kao i obrada od strane tijela koja podliježu GDPR-u, LED-u ili drugim EU institucijama. Svi navedeni obuhvaćeni su općim jamstvom zaštite osobnih podataka propisanim čl. 16 Ugovora o funkcioniranju Europske unije (UFEU):

> Članak 16.
>
> 1. Svatko ima pravo na zaštitu svojih osobnih podataka.
> 2. Europski parlament i Vijeće, odlučujući u skladu s redovnim zakonodavnim postupkom, utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu osobnih podataka u institucijama, tijelima, uredima i agencijama Unije te u državama članicama kad obavljaju svoje aktivnosti u području primjene prava Unije i pravila o slobodnom kretanju takvih podataka. Poštivanje tih pravila podliježe nadzoru neovisnih tijela. Međutim, navedeno se ne odnosi na obradu osobnih podataka od strane ZVSP tijela spomenutih prethodno, iz razloga što nakon navedenog teksta članka, zadnja rečenica istog glasi ovako:

Pravila usvojena na temelju ovog članka ne **dovode u pitanje posebna pravila** utvrđena u članku 39. Ugovora o Europskoj uniji.

Kasniji članak Ugovora o Europskoj uniji propisuje sljedeće:

> Članak 39.
>
> U skladu s člankom 16. Ugovora o funkcioniranju Europske unije i odstupajući od njegova stavka 2., **Vijeće usvaja odluku u kojoj se utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu osobnih podataka od strane država članica pri obavljanju aktivnosti u području primjene ovog poglavlja** [tj. u odnosu na ZVSP] i pravila o slobodnom kretanju takvih podataka. Poštivanje tih pravila podliježe nadzoru neovisnih tijela.

Ovo nije mjesto za daljnju raspravu o predmetnoj temi.[192] Dovoljno je napomenuti kako se na području

190 Popis s poveznicama na svaki pojedini instrument ili aktivnost, vidi web stranicu navedenu prethodnoj bilješci.
191 Usp. mišljenja i komentara ENZP-a u odnosu na takva pitanja, navedena ovdje: https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en
192 Za daljne pojašnjenje vidi: Pismo EDPS od 23. srpnja 2007. Međunarodnoj konferenciji o zaštiti podataka sukladno Reformskom ugovoru (kako je tijekom izrade nacrta bio nazvan Lisabonski ugovor) - EDPS Zajedničko mišljenje o obavijestima za prethodnu provjeru zaprimljeno od službenika za zaštitu podataka Vijeća EU u odnosu na obradu osobnih podataka u svrhu provođenja restriktivnih mjera u vezi zamrzavanja imovine, Brisel, 07. svibnja 2014. (2012-0724, 2012-0725, 2012-0726), str. 10, dostupno na: https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf

ZVSP-a, primjenjuje propis koji se odnosi na obradu osobnih podataka od strane EU institucija (itd.), Uredba 2018/1725, objašnjena u sljedećem poglavlju – ali samo u ograničenom opsegu; te da je za posebna pravila zaštite podataka koja se odnose na svaku aktivnost obrade podataka u kontekstu ZVSP-a, uključujući predmete nadležnost tijela za zaštitu podataka kao i obvezu imenovanja SZP-a, važno znati konkretnu odluku Vijeća koja se na to odnosi.

1.4.5. Zaštita podataka za EU institucije: nova uredba

Kako je navedeno u odlomku 1.3.6, prethodno, prvi EU instrument za zaštitu podataka u odnosu na obradu osobnih podataka od strane samih EU institucija, Uredba 45/2001, stavljena je van snage Uredbom (EU) 2018/1725, koja je stupila na snagu **11. prosinca 2018.**[193] (uz određene **iznimke** i određena **kašnjenja u primjeni,** kako je navedeno pod naslovima u nastavku).

DVA REŽIMA

Izuzev navedenih iznimki i kašnjenja, Uredba 2018/1725 zapravo je kreirala **dva odvojena režima zaštite podataka:** jedan se odnosio na sve ***EU institucije i tijela koja nisu uključena u policijsku i pravosudnu suradnju*** te jedan koji se odnosi na ***EU institucije i tijela koja su uključena u predmetnu suradnju*** (vidi čl. 2, st. 1 i 2)

Režim zaštite podataka primjenjiv na EU institucije i tijela koja nisu uključena u policijsku i pravosudnu suradnju:

Predmetni režim, utvrđen u poglavljima I do VIII nove uredbe, **u većem dijelu je jednak režimu uspostavljenom Općom uredbom o zaštiti podataka (GDPR)** za obradu koja podliježe zadnjem instrumentu. Dakle, Uredba 2018/1725 kao i GDPR, obuhvaća novo načelo "**odgovornosti**" (čl. 4(2); usp. također čl. 26) te utvrđuje **obveze voditelja i izvršitelja obrade (Poglavlje IV), na jednako učinkovit način kao što to za voditelje i izvršitelje obrade određuje GDPR.**

Konkretno, Poglavlje IV uključuje i odredbe o načelu "**tehničke i integrirane zaštite podataka"** (čl. 27); o dogovorima koji će se uspostaviti u odnosu na "**zajedničke voditelje obrade"** (čl. 28.), **izvršitelje** (čl. 29.) te **osobe koje djeluju pod nadležnošću voditelja ili izvršitelja obrade** (čl. 30); o (s "odgovornošću" povezanom) obvezi čuvanja detaljne **evidencije aktivnosti obrade** (čl. 31.); o **sigurnosti obrade** (čl. 33), **obavijesti o povredi podataka Europskom nadzorniku za zaštitu podataka (ENZP)** (koji je ujedno i nadzorno tijelo u odnosu na EU institucije i tijela) (čl. 34) te o **obavješćivanju ispitanika o povredi podataka** (čl. 35) – jednako kako to propisuje i GDPR.

Uredba 2018/1725 (kao i prethodna, Uredba 45/2001, o kojoj je riječ u odjeljku 1.3.6, iznad) zahtijeva od svake institucije ili tijela Unije imenovanje **službenika za zaštitu podataka (SZP)** (čl. 43) – što je ponovno jednako u odnosu na GDPR u dijelu voditelja obrade u javnom sektoru. Odredbe o **položaju SZP-a** (čl. 44) te **obvezama** istog (čl. 45) također su jednake kao u GDPR-u, uz **dodatne odredbe** u odnosu na dostupnost SZP-a svima te zaštitu od eventualne štete zbog određenog činjenja (čl. 44(7)) kao i o trajanju imenovanja SZP-a (čl. 45(8)); a u odnosu na zadaće SZP-a, nešto je snažnija odredba (koja se ne nalazi u GDPR-u) da SZP "*na neovisan način osigurava internu primjenu ove Uredbe"* (čl. 45(1)(b)).[194]

193 Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. kolovoza 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ, SL L 295, 21. studenog 2018., str. 39-98, dostupna na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

194 Navedeno je snažnije, iako GDPR propisuje da "*su voditelj i izvršitelj obrade dužni osigurati službeniku za zaštitu samostalnost u odlučivanju, da ne prima upute o izvršenju svojih zadaća"* te "*da on ili ona ne smiju biti otpušteni ili kažnjeni od strane voditelja ili izvršitelja obrade zbog izvršavanja svojih zadaća"* (čl. 38(3) GDPR-a), što osigurava da SZP može djelovati "neovisno", GDPR ističe kako SZP mora "nadgledati usklađenost [GDPR-a i drugih relevantnih pravila] te "*informirati i savjetovati"* voditelja obrade i zaposlenike (i eventualne izvršitelje obrade) o njihovim obvezama (čl. 39(1)(b) i (a)), i GDPR ne zahtijeva od SZP da "osigura" internu usklađenost, dok zakonska odgovornost ostaje na voditelju obrade.

Uredba 201/1725 također zahtijeva provođenje **procjene učinka na zaštitu podataka (PUZP),** pod jednakim uvjetima kako je to predviđeno GDPR-om, tj. u odnosu na obradu "koja bi vjerojatno rezultirala visokim rizikom za prava i slobode ispitanika" (čl. 39); te propisuje nužnost "**prethodnih konzultacija"** s ENZP-om pod jednakim uvjetima kako je to određeno u odnosu na nadležna nadzorna tijela u GDPR-u, tj. ukoliko PUZP pokaže kako se takvi rizici ne mogu u dovoljnoj mjeri ublažiti (čl. 40) (posljednja rečenica korisno dodaje kako "*Voditelj obrade treba zatražiti savjet službenika za zaštitu podataka o potrebi za prethodnim savjetovanjem*" – ali to je, naravno, preporučljivo i u odnosu na obradu sukladno GDPR-u).

Što se tiče materijalnog sadržaja, Uredba 2018/1725 se također temelji na jednakim ***definicijama*** (čl. 3) i ***temeljnim načelima*** (čl. 4) kao i GDPR te sadrži zapravo ista pravila o pitanjima kao što su ***suglasnost/privola i drugi pravni temelji za obradu neosjetljivih i osjetljivih podataka*** (usp. čl. 5 – 13), ali uz dodatne detalje o "**usklađenoj obradi**" (čl. 6) i ***prijenosu osobnih podataka primateljima u zemljama članicama*** (čl. 9.);[195] i o ***pravima ispitanika*** (čl. 14 – 24), te **automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila** (čl. 24).

Također predviđa u osnovi jednaka dopuštena **ograničenja prava ispitanika i obveza obavješćivanja ispitanika o povredi podataka** (čl. 25(1)), ali ih proširuje na ***obvezu osiguranja povjerljivosti elektroničkih komunikacija*** (navedeno niže) i, što je još važnije, utvrđuje konkretnija pravila o tome što ***"pravni akt ili interno pravilo"*** kojim se predviđaju ovakva ograničenja treba posebno pojasniti (vidi čl. 25(2)). Štoviše, u vezi nacrta takvih pravila potrebne su konzultacije s Europskim nadzornikom za zaštitu podataka (čl. 41(2)), koji predstavlja jamstvo da će predmetna pravila zaista biti ograničena na ono što je "*nužno i proporcionalno... u demokratskom društvu*".

Uredba 2018/1725 obuhvaća i poseban odlomak (Poglavlje IV, odlomak 3) o **povjerljivosti elektroničkih komunikacija.** Isti propisuje da će

> Institucije i tijela Unije **osigurati povjerljivost elektroničkih komunikacija** osiguravanjem njihovih elektroničkih komunikacijskih veza (čl. 36, dodatno naglašeno) -

te da će:

> zaštititi podatke koji su preneseni, pohranjeni, povezani, obrađeni i prikupljeni s terminalne opreme korisnika koji pristupaju njihovim javno dostupnim web stranicama i mobilnim aplikacijama, sukladno članku 5(3) Direktive 2002/58/EC [tj. Direktive o e-privatnosti, o kojoj se govori u odlomku 1.3.3., iznad] (čl. 37, dodatno naglašeno).

Posljednji članak u ovom odjeljku odnosi se na **korisničke imenike,** kako je definirano člankom 3(24), tj. na sve:

> javno dostupne imenike korisnika ili unutarnje imenike korisnika dostupne unutar institucija ili tijela Unije ili podijeljene između institucija i tijela Unije, bez obzira jesu li u tiskanom ili elektroničkom obliku.

U tom pogledu u članku 38. propisano je da osobni podaci sadržani u takvim imenicima moraju biti "*ograničeni na ono što je zbilja nužno za ispunjenje svrhe imenika*" (čl. 38(1)) te da institucije i tijela moraju:

> poduzeti sve potrebne mjere kako bi spriječili da se osobni podaci sadržani u tim imenicima, bez obzira na to jesu li dostupni javnosti ili nisu, upotrebljavaju u svrhu izravnog marketinga.

195 Vidi pododlomak 1.4.6., niže.

Pravila navedena u ovom odjeljku odražavaju neka pravila Direktive o e-privatnosti, o kojoj je bilo riječi u odjeljku 1.3.3., iznad.

Pravila o **prijenosu osobnih podataka u treće zemlje i međunarodne organizacije,** sadržana u Poglavlju V Uredbe 2018/1725 ponovno slijede iste odredbe sadržane i u GDPR-u: takvi prijenosi mogu se izvršiti samo:

- na temelju **odluke o primjerenosti** koju izdaje Komisija sukladno GDPR-u;

ili

- ukoliko su **"odgovarajuće zaštitne mjere"**:
  - pravno obvezujući i provedivi instrumenti između javnih tijela ili tijela;
  - standardne klauzule o zaštiti podataka koje je usvojila Komisija;
  - standardne klauzule o zaštiti podataka koje je usvojio ENZP i odobrila Komisija;
  - u odnosu na prijenose izvršitelju obrade koji nije institucija ili tijelo Unije: Obvezujuća korporativna pravila (OKP), kodeksi ponašanja ili certifikati sukladno GDPR-u; ili podliježe odobrenju ENZP-a:
  - o ugovorne klauzule između nadležnih tijela; ili
  - odredbe o zaštiti podataka umetnute u administrativne sporazume između javnih tijela ili tijela (čl. 48)

Uredba 2018/1725 također sadrži odredbu, sličnu onoj u GDPR-u, koja glasi:

> Sve presude suda ili sve odluke upravnog tijela treće zemlje kojima se od voditelja obrade ili izvršitelja obrade zahtijeva prijenos ili otkrivanje osobnih podataka mogu biti priznate ili izvršive na bilo koji način samo ako se temelje na nekom međunarodnom sporazumu (čl. 49).

Naposljetku, u tom pogledu, članak 50. Uredbe 2018/1725 predviđa prijenos na temelju "**odstupanja za posebne situacije**", na isti način kako je to predviđeno GDPR-om, tj. kada je ispitanik **"izričito pristao"** na predloženi prijenos (čl. 50(1)(a)), ili kada je prijenos **"nužan"** u ***ugovornom kontekstu*** (čl. 50(1)(b) i (c)), zbog ***važnih razloga od javnog interesa prepoznatog od strane zakonodavstva Unije*** (čl. 50(1)(d) zajedno s čl. 50(3)), za uspostavljanje, izvršavanje ili obranu ***pravnih zahtjeva*** (čl. 50(1)(e)) ili za zaštitu ***temeljnih interesa ispitanika ili drugih osoba,*** u slučaja kada je ispitanik fizički ili pravno nesposoban dati pristanak (čl. 50(1)(f)); ili kada je prijenos izvršen iz **javno dostupnog registra** (pod uvjetom da su ispunjeni svi uvjeti za pristup) (čl. 50(1)(g)).

Uredba 2018/1725, kao i GDPR u odnosu na javna tijela, propisuje da se prva tri od navedenih odstupanja (izričita suglasnost ispitanika; ugovorni kontekst) "*ne primjenjuju na aktivnosti koje obavljaju institucije i tijela Unije prilikom izvršenja njihovih javnih ovlasti*" (čl. 50(2)).

Poglavlje VI Uredbe 2018/1725 obuhvaća **uspostavu, pravila, pozicije, zadaće i obveze ENZP-a.** U osnovi, ENZP ispunjava istu funkciju, u odnosu na obradu osobnih podataka od strane institucija i tijela, kao i nadležna tijela (tijela za zaštitu podataka, TZP) uspostavljena sukladno GDPR-u u odnosu na obradu osobnih podataka od strane odgovarajućih nacionalnih javnih tijela država članica (ili regije države članice) za koju su nadležni.

Poglavlje VII obuhvaća **suradnju između i koordiniranog nadzora od strane Europskog nadzornika za zaštitu podataka i nacionalnih nadležnih tijela.** Uredba također, ponovno kao i GDPR, **potiče suradnju s trećim zemljama i međunarodnim organizacijama** za zaštitu osobnih podataka (čl. 51).[196]

Zaključno, Poglavlje VIII se bavi **pravnim lijekovima, odgovornošću i kaznama,** koje su ponovno jednake onima iz GDPR-a. Dovoljno je napomenuti da svaki ispitanik čiji se osobni podaci obrađuju od strane institucija ili tijela EU može podnijeti pritužbu ENZP-u (čl. 63) (kao što se svaki ispitanik može žaliti odgovarajućem nacionalnom tijelu za zaštitu podataka, sukladno GDPR-u) te (opet kao i u GDPR-u) ima pravo na naknadu za

196 Kao i u GDPR-u, odgovarajuća odredba (čl. 50 u GDPR-u) pomalo je čudno postavljena u poglavlju o prijenosu podataka, a ne u onom o zadaćama i ovlastima nadzornih tijela.

svu materijalnu ili nematerijalnu štetu uzorkovanu kršenjem Uredbe (čl. 65). Štoviše, kao i sukladno GDPR-u ispitanici u takvim slučajevima mogu biti zastupani od strane neprofitnih organizacija aktivnih u pogledu os

obnih podataka (čl. 67) – na koje se dalje dodaje odredba o pritužbama osoblja EU (čl. 68). Nasuprot tome, svaki dužnosnik EU koji ne poštuje obveze propisane Uredbom podliježe disciplinskim mjerama (čl. 69). **Sud Europske unije nadležan je** za svaki spor u odnosu na Uredbu, uključujući naknadu štete (čl. 64). Također, **ENZP može izreći upravno novčane kazne** institucijama i tijelima EU koje ne provode Uredbu (čl. 66) (iako je razina novčanih kazni mnogo niža u odnosu na one predviđene GDPR-om).[197]

S obzirom na to da je glavni režim zaštite podataka sukladno Uredbi 2018/1725 vrlo usko usklađen s GDPR-om – često vrlo detaljno i praktično – smjernice i stajališta koje izdaje Europski nadzornik za zaštitu podataka institucijama i tijelima EU koji podliježu tom režimu također će biti od izravne važnosti za voditelje obrade osobnih podataka sukladno GDPR-u, posebno u javnom sektoru te ga stoga trebaju detaljno proučiti svi SZP-ovi zaposleni kod takvog voditelja obrade (zajedno, naravno, sa smjernicama i mišljenjima Europskog odbora za zaštitu podataka čiji je i ENZP član; stajališta ENZP-a i EOZP-a se razmjenjuju.

Režim zaštite podataka koji se primjenjuje na institucije i tijela EU koja sudjeluju u policijskoj i pravosudnoj suradnji:

Općenito:

Kako je prethodno navedeno, Uredba 2018/1725 stvara **zaseban režim zaštite podataka za institucije i tijela EU koja sudjeluju u policijskoj i pravosudnoj suradnji** (tj. koja su uključena u "*aktivnosti iz opsega Poglavlja 4 ili Poglavlja 5 glave V trećeg dijela UFEU*"). Ovaj zasebni režim utvrđen je u **Poglavlju IX Uredbe,** koji obuhvaća članke 70 – 95 (pri čemu članak 2(2) jasno navodi da su **definicije** utvrđene u članku 3. također primjenjive u ovom poglavlju).[198]

Poseban režim uređuje obradu od strane odgovarajućih institucija ili tijela "**operativnih osobnih podataka".** Navedeno je definirano u članku 3(2) kao:

> Svi osobni podaci koje obrađuju tijela, uredi ili agencije pri obavljanju aktivnosti obuhvaćenih područjem primjene trećeg dijela glave V. poglavlja 4. ili 5. UFEU kako bi se ispunili ciljevi i zadaće utvrđeni u pravnim aktima o osnivanju tih tijela, ureda ili agencija.

U osnovi, obrada takvih osobnih podataka podliježe posebnom režimu u Poglavlju IX, dok obrada svih "neoperativnih" osobnih podataka – kao što su podaci o ljudskim resursima koji se odnose na osoblje određenih institucija i tijela – podliježe glavnom režimu utvrđenom u ranijim poglavljima Uredbe 2018/1725, kako je opisano u prethodnom podnaslovu.

U okviru prethodnog podnaslova, utvrdili smo pravila za glavni režim usko usklađen s GDPR-om. Isto tako, pravila iz poglavlja IX Uredbe 2018/1725 često su u skladu s Direktivom o zaštiti podataka u provedbi zakona (LED), o kojima se raspravlja u odjeljku 1.4.3. iznad (ili s obje direktive i GDPR-om te pravilima glavnog

197 Maksimalna kazna koju ENZP može izreći institucijama ili tijelima EU za neusklađenost s Uredbom 2018/1725, pojedinačno je 25.000 € do ukupno 250.000 € godišnje za neke povrede te 50.000 € po povredi i do ukupno 500.000 € godišnje za neke druge povrede (vidi čl. 66(2) i (3)). To se uspoređuje s upravno novčanim kaznama do 10.000.000 € ili u slučaju poduzetnika (privatnog društva) do 2% ukupnog godišnjeg prometa (ovisno o tome što je više viši) za određene povrede te do 20.000.000 € ili u slučaju poduzetnika, do 4% ukupnog godišnjeg prometa (ovisno o tome što je više) za druge povrede, koje su nametnute GDPR-om (čl. 83(4) i (5) - iako GDPR također omogućuje državama članicama da smanje navedene iznose ili da čak u potpunosti isključuju javna tijela i tijela s poslovnim nastanom na njihovom teritoriju od upravno novčanih kazni (čl. 83(7)) (ali takva tijela koja su oslobođena od upravno novčanih kazni ili podliježu smanjenim novčano upravnim kaznama moraju i dalje podlijegati ovlastima nadležnih tijela za zaštitu podataka u skladu s člankom 58(2) GDPR-a).

198 Na pitanje primjenjuju li se i u kojoj mjeri poglavlja VII I VIII na obradu u okviru Poglavlja IX, vidi niže, pod naslovom "*Prava, nadzor i provedba*".

režima u skladu s Uredbom 2018/1725) – ali poglavlje IX nije baš usko usklađeno s LED-om kao što je glavni režim s GDPR-om. Stvari mogu biti poprilično zamršene.[199]

S obzirom na to da je ovaj priručnik namijenjen SZP-ima javnih tijela država članica, pojedinosti o podudarnosti ili razlikama između pravila iz Poglavlja IX i onih u prethodnom dijelu Uredbe 2018/1725 – i onih iz glavnih instrumenata EU za zaštitu podataka, GDPR i LED – nije potrebno raspravljati u ovom dijelu. Međutim, dva posebna pitanja mogu se napomenuti u sljedećim pododlomcima.

Prava, nadzor i provedba:

U poglavlju IX **nema navedenog** prava ispitanika na **naknadu štete prouzročenu protupravnom obradom** (što bi značilo obradu suprotnu odredbama predmetnog poglavlja), s pravom ispitanika da bude **predstavljen** od strane neprofitnih tijela ili ovlasti ENZP-a za izricanje **administrativnih kazni**.

Odredbe poglavlja IX opetovano spominju obvezu voditelja obrade iz poglavlja IX, za informiranjem ispitanika o njihovim pravima ulaganja pritužbe ENZP-u (vidi čl. 79(2)(d), 80(f) i 81(2)) te mogućnost ulaganja pravnih lijekova prije Suda (čl. 81(2)). Voditelji obrade sukladno Poglavlju IX također mogu dogovoriti da se prava ispitanika u određenim slučajevima "obavljaju putem Europskog nadzornika za zaštitu podataka" (čl. 84(1)) tj. samo neizravno, i u tom slučaju moraju:

> Informirati ispitanika o mogućnosti ostvarivanja njegovih prava preko Europskog nadzornika za zaštitu podataka sukladno stavku 1. (čl. 84(2)).

Voditelj obrade je također dužan bilježiti **logove** obrade te ih učiniti dostupnim ENZP-u na zahtjev (čl. 88(3)) te **obavijestiti ENZP** o kršenju osobnih podataka (čl. 92(1) i (4)).

Međutim, iz članka 2(2) jasno proizlazi da se poglavlje Uredbe koje predviđa postupak pritužbi ENZP-a, nadležnost Suda EU te djelovanje ENZP-a, također u slučajevima kršenja osobnih podataka (Poglavlje VIII) i poglavlje koje zapravo navodi obveze i ovlasti ENZP-a u tom pogledu (Poglavlje VI) ne primjenjuju na obradu operativnih podataka koji podliježu samo Poglavlju IX.

Čini se kako, u praksi, ENZP preuzima nadzorne i savjetodavne ovlasti, također u odnosu na obradu operativnih osobnih podataka od strane institucija i tijela EU koji podliježu Poglavlju IX Uredbe 2018/1725 te će biti voljan prihvatiti pritužbe ispitanika u odnosu na takvu obradu. Hoće li dopustiti ispitanicima da u predmetnim slučajevima budu predstavljeni od strane nevladinih organizacija ili će biti voljan naložiti naknadu ili čak izreći administrativnu kaznu određenim institucijama i tijelima – te bi li Sud odobrio takvu praksu izvršavanja ovlasti ENZP-a u odnosu na takvu obradu – ostaje za vidjeti.

Odstupanja i odgođena provedba Uredbe 2018/1725

U načelu, Uredba 2018/1725 primjenjuje se na svu obradu osobnih podataka od strane institucija i tijela Unije (čl. 2(1)) – iako, kako smo vidjeli, stvaranjem dvaju pravnih režima. Međutim, Uredba sadržava i određena odstupanja od primjene te predviđa odgodu provedbe odredbi u određenim slučajevima, kako je sljedeće objašnjeno.

Izuzeća:

Članak 2(4) propisuje da se:

199 Samo jedan primjer: blisko povezan s novim načelom "**odgovornosti**" koji se primjenjuje na sve moderne instrumente zaštite podataka EU, dužnost je voditelja obrade da zadrži zapise i dnevnike. Međutim, GDPR i pravila koja se primjenjuju na glavni režim u skladu s Uredbom 2018/1725 zahtijevaju čuvanje detaljnih zapisa svih aktivnosti obrade (čl. 30. GDPR; čl. 31 Uredbe 2018/1725), ali ne zahtijevaju čuvanje dnevnika/logova. LED zahtijeva i detaljne zapise i detaljne logove/dnevnike (čl. 24. I 25). Međutim, Poglavlje IX Uredbe 2018/1725 zahtijeva samo čuvanje logova odnosnih na obradu operativnih osobnih podataka (čl. 88.), bez spominjanja zapisa.

Ova Uredba ne primjenjuje na obradu osobnih podataka u misijama iz čl. 42(1) i čl. 43 i 44 UEU-a (dodatno naglašeno).

Misije i zadaci obuhvaćeni izuzećem su:

- misije izvan Unije u svrhu održanja mira, sprječavanja sukoba ili osnaživanja međunarodne sigurnosti u skladu s odredbama povelje Ujedinjenih naroda (čl. 42(1))
- zajednički poslovi razoružanja, humanitarne i spasilačke zadaće, vojni savjeti i pomoć, sprječavanje sukoba i zadaće održanja mira, zadaće borbenih snaga u upravljanju krizom, uključujući uspostavu mira i post-konfliktnu stabilnost. Sve navedene zadaće (čl. 43 koji se proširuje na čl. 44).

Druga rečenica članka 43 dodaje kako sva djelovanja i zadaće navedene u tom članku "*mogu doprinijeti borbi protiv terorizma, uključujući potporu trećim zemljama u borbi protiv terorizma na njihovom teritoriju*".

Odgođena provedba:

Osim prethodno navedenog, izuzeća primjene Uredbe u odnosu na posebne operacije za koje se mogu odrediti posebna pravila, Uredba također utvrđuje proces provođenja obrade od strane nekih institucija i tijela EU u skladu s Uredbom 2018/1725, s rokovima za određeno preispitivanje (ali ne i za stvarno usklađenje predmetnih operacija s Uredbom). Posebno, prije svega, članak 2(3) propisuje da:

> Se ova Uredba ne primjenjuje na obradu operativnih osobnih podataka koju provode **Europol i Ured europskog javnog tužitelja**, do usvajanja [propisa iz vremena prije Lisabonskog ugovora koji obuhvaćaju njihovo djelovanje][200] u skladu s člankom 98 ove Uredbe.

Također, članak 98. propisuje da:

1) do 30. travnja 2022. Komisija preispituje pravne akte donesene na temelju Ugovora kojima se uređuje obrada operativnih osobnih podataka koju obavljaju tijela, uredi ili agencije Unije pri obavljanju aktivnosti obuhvaćenih područjem primjene trećeg dijela, glave V. poglavlja 4. ili 5. TFU-a, kako bi se:
   a. ocijenila njihova usklađenost s Direktivom (EU) 2016/680 i poglavljem IX ove Uredbe;
   b. utvrdila sva odstupanja koja bi mogla omesti razmjenu operativnih osobnih podataka između tijela, ureda i agencija Unije pri obavljanju aktivnosti u tim područjima i nadležnih tijela; te
   c. utvrdila odstupanja koja bi mogla dovesti do pravne rascjepkanosti zakonodavstva o zaštiti podataka u Uniji.
2) Na temelju tog preispitivanja, kako bi se zajamčila ujednačena i dosljedna zaštita pojedinaca u vezi s obradom, Komisija može podnijeti odgovarajuće zakonodavne prijedloge, posebno radi primjene poglavlja IX ove Uredbe na Europol i Ured europskog javnog tužitelja i uključujući prilagodbe poglavlja IX ove Uredbe, ako je to potrebno.

Drugim riječima, uredbe koje obuhvaćaju **djelovanje Europola i UEJT-a** te ostalih institucija i tijela koja podliježu članku 98., moraju se **preispitati do 30. travnja 2022.,** nakon čega Komisija može **predložiti** nova pravila u odnosu na obradu osobnih podataka od strane tih tijela u skladu s LED-om (navedeno u odjeljku 1.4.3, iznad) te posebnim pravilima iz poglavlja IX Regulative (navedeno iznad). Međutim, nije određen **datum** do kojeg se predmetna nova pravila trebaju usvojiti, što će zahtijevati zakonodavno djelovanje Vijeća ministara i eventualno novog Europskog parlamenta te pribavljanje mišljenja Europskog nadzornika za

200 Odnosno: Uredba (EU) 2016/794 Europskog parlamenta i Vijeća od 11. svibnja 2016. o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol) te zamjeni i stavljanju izvan snage odluka Vijeća 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP te Uredba Vijeća (EU) 2017/1939 od 12. listopada 2017. o provedbi pojačane suradnje u vezi s osnivanjem Ureda europskog javnog tužitelja (EPPO), SL L 283, 31. listopada 2017., str. 1.

zaštitu podataka i Europskog odbora za zaštitu podataka – što zahtijeva i protok određenog vremena. Dok se ti propisi ne izmijene u potpunosti – tj. barem nekoliko sljedećih godina – obrada osobnih podataka od strane Europola i UEJT-a (te ostalih tijela i institucija iz članka 98 Regulative 2018/1725) ostat će pod vlastitim trenutnim (prije 2018.) pravilima o zaštiti podataka.

1.4.6. Prijenos osobnih podataka između različitih režima zaštite podataka EU

I. RAZLIČITI REŽIMI ZAŠTITE PODATAKA

Iz različitih prethodnih odjeljaka bit će jasno kako postoji znatan broj različitih, općih ili specifičnih režima zaštite podataka u glavnim instrumentima i okvirima EU zaštite podataka, a neki i izvan tih (čak i izvan prava EU), uključujući one utvrđene u nastavku. Koji se režimi primjenjuju na određenu aktivnost ili proces obrade ovisit će o procjeni svake pojedine aktivnosti i procesa i njihovih posebnih svrha, a posebno o tome je li stvar pod nadležnošću EU ili ne, bilo da se odvija u privatnom ili javnom sektoru, uključuje li EU ili nacionalne institucije koje djeluju u odnosu na gospodarska ili kaznena pitanja itd.

Opća uredba o zaštiti podataka:

- GDPR režim koji se primjenjuje na obradu od strane privatnih subjekata
- GDPR režim koji se primjenjuje na obradu od strane javnih subjekata koji nisu uključeni u kaznenopravna ili pitanja javne sigurnosti ili pitanja nacionalne sigurnosti (pri čemu se "javna sigurnost" shvaća kao vrlo ograničena kategorija). **Direktiva o e-privatnosti/predložena Uredba o e-privatnosti**
- Posebna pravila koja se primjenjuju na pružatelje usluga e-komunikacije (i u budućnosti drugi pružatelji kao što su OTT igrači)
- Posebna pravila koja se primjenjuju na sve web-poslužitelje (uključujući javna tijela s vlastitim web stranicama) u odnosu na povjerljivost komunikacija, korištenje "kolačića" itd.

Direktiva o zaštiti podataka u provođenju zakona:

- LED se primjenjuje na javne subjekte (nadležna tijela) kada obrađuju osobne podatke "u svrhu sprječavanja, istrage, otkrivanja ili kaznenog progona kaznenih djela ili izvršenja kaznenopravnih sankcija, uključujući suzbijanje i sprječavanje prijetnji javnoj sigurnosti", bilo kao njihov glavni zadatak ili povremeni, osim drugih javnih zadaća.

Područja izuzeta od primjene LED-a (od samog početka):

- Pravila o približno 123 pravna instrumenta EU koja se odnose na ono što se nekad zvalo pitanja "pravosuđe i unutarnji poslovi" (PUP) koja su stupila na snagu prije 6. svibnja 2016. (koje se nastavljaju primjenjivati iako nisu usklađene s LED-om).
- Pravila u "međunarodnim sporazumima koji uključuju prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama, sklopljenim s državama članicama prije 6. svibnja 2016. i koja su u skladu s pravom Unije koje je primjenjivo prije navedenog datuma" (koja se također nastavljaju primjenjivati iako još nisu u potpunosti usklađena s LED-om).
- Pravila o korištenju "automatiziranih sustava obrade postavljena prije 6. svibnja 2019." u državama članicama, ukoliko još nisu usklađena s LED-om jer bi to prouzročilo "*nesrazmjeran napor*".

Obrada osobnih podataka iz područja ZVSP-a:

- Obrada od strane Visokog predstavnika EU za vanjske poslove i sigurnosnu politiku, Europske službe za vanjsko djelovanje (ESVD) i 141 EU delegacije diljem svijeta te usluga Instrumenata vanjske politike (FPI) i obrada od strane država članica u odnosu na predmetna pitanja (uključujući usvajanje Odluke Vijeća o području ZVSP-a) – koji još uvijek nisu predmet nekog određenog EU instrumenta zaštite podataka. [No zabilježite treću uvlaku ispod sljedećeg naslova].

Obrada osobnih podataka od strane EU institucija i tijela sukladno Uredbi 2018/1725:

- Režim zaštite podataka koji se primjenjuje na EU institucije i tijela koja nisu uključena u policijsku i pravosudnu suradnju.
- Režim zaštite podataka koji se primjenjuje na EU institucije i tijela koji sudjeluju u policijskoj i pravosudnoj suradnji.
- Obrada od strane tajništva Vijeća u provedbi Odluke ZVSP Vijeća – ograničeno područje aktivnosti u odnosu na ZVSP koja podliježu pravilima zaštite podataka, tj. Uredbi 2018/1725.

Područja izuzeta od primjene Uredbe 2018/1725 (od početka):

- Obrada osobnih podataka u okviru misija EU usmjerenih na očuvanje mira, sprječavanje sukoba i osnaživanje međunarodne sigurnosti ili zaduženja u sklopu zajedničkih operacija razoružanja, humanitarnih zadaća i zadaća spašavanja, zadaća vojnog savjetovanja i pomoći, zadaća sprječavanja sukoba i održanja mira, zadaća borbenih snaga u upravljanju kriznim situacijama, uključujući izgradnju mira i stabilizaciju nakon sukoba (i kada se takvi zadaci odnose na borbu protiv terorizma, uključujući podršku trećim zemljama u borbi protiv terorizma na njihovom teritoriju).
- Obrada osobnih podataka od strane Interpola i Ureda europskog javnog tužitelja (UEJT) te drugih "tijela, ureda i agencija Unije pri obavljanju zadaća koje podliježu opsegu poglavlja 4 ili poglavlja 5., glave V. trećeg dijela UFEU [tj. koji se odnose na policijsku i pravosudnu suradnju]", koja će se nastaviti odvijati temeljem pravnih instrumenata EU koji se odnose na Interpol ili UEJT ili na drugi oblik policijske i pravosudne suradnje, usvojenu prije Uredbe 2018/1725.

Nacionalna sigurnost:

- Obrada osobnih podataka od strane država članica u odnosu na nacionalnu sigurnost – koja je u cijelosti izvan područja primjene prava EU, zapravo čak i Povelje o temeljnim pravima (iako takva obrada, naravno, podliježe Europskoj konvenciji o ljudskim pravima te nadležnosti Europskog suda za ljudska prava).[201]

Nije uvijek lako povući jasne linije između različitih režima, npr. između policijskog djelovanja u prevenciji kriminala, policijskog djelovanja u osiguravanju reda, policijskog djelovanja i djelovanja drugih tijela u odnosu na "unutarnju sigurnost", "javnu sigurnost" te "nacionalnu sigurnost", kao i između takvih djelovanja i djelovanja EU u odnosu na "terorizam"[202], gore navedenim zadaćama EU i "međunarodne sigurnosti".

Ovo nije mjesto za detaljniju analizu razlika. Dovoljno je napomenuti, kada se različiti režimi primjenjuju na različite aktivnosti (aktivnosti koje spadaju u više od jedne gore navedene kategorije), možda čak i od strane istih subjekata, bit će važno za određene sudionike, kao voditelje obrade (i često kao izvršitelje obrade, tj. kada podržavaju druge takve aktere) razjasniti koje pravne režime primjenjuju na koju vrstu obrade osobnih podataka, analizirajući svaki zasebno proces obrade. Zakonitost obrade i opseg izuzeća u tako važnim pitanjima kao što su prava ispitanika, uvelike ovise o navedenim pojašnjenjima.

201 Europski sud za ljudska prava izdao je nekoliko važnih presuda u tom pogledu. Vidi: Istraživački odjel Europskog suda za ljudska prava, Nacionalna sigurnost I Europska sudska praksa, VIjeće Europe, 2013., dostupno na: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf Međutim, navedeno se ne može primijeniti od strane EU institucija u odnosu na takve aktivnosti.

202 Usp. John Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?" u: Utrecht Law REview, VOlume 1, Issue 1 (Listopad 2005), dostupno na: http://www.utrechtlawreview.org/

Javna tijela uključena u različite aktivnosti koje su predmet različitih režima zaštite podataka, trebaju uvijek pažljivo razgraničiti svoje različite aktivnosti, različite načine obrade te različite osobne podatke koji se koriste u različitim postupcima obrade te evidencijama o aktivnosti obrade kao i procjeni takve obrade.[203] Službenici za zaštitu podataka u takvim javnim tijelima imaju ključnu ulogu u tom pogledu.[204]

II. PRIJENOS OSOBNIH PODATAKA

Posebna pitanja se pojavljuju kada se predloži ili zahtijeva da se osobni podaci, prikupljeni u jednu određenu svrhu sukladno pravilima jednog od prethodno spomenutih režima, od istog voditelja obrade koriste u drugu svrhu, za obradu sukladno drugom pravnom režimu; ili da budu proslijeđeni ili na neki drugi način dostupni drugom tijelu (drugom voditelju obrade) za neku drugu svrhu i obradu sukladnu drugom pravnom režimu.[205]

Na primjer, obrazovni odjel na lokalnoj razini može prikupljati osobne podatke o učenicima u obrazovne svrhe sukladno GDPR-u, međutim lokalna policija može zatražiti pristup (nekim od) tih podataka u svrhu rješavanja kriminala na lokalnoj razini (npr. kako bi provjerili koji učenici su određenog dana bili odsutni s nastave). Predložena obrada podataka za drugu svrhu bila bi u nadležnosti LED-a (ili preciznije rečeno, nacionalnog zakona u koji su prenesene odredbe LED-a, kao i pod nadležnošću određenih zakona odnosnih na policijske i kaznene postupke). Ponekad, primjenjivi zakoni ili zakonska pravila pojašnjavaju kada se takvi uvidi mogu izvršiti (npr. samo u vezi određenih zločina ili ukoliko postoji opravdana sumnja prema određenoj djeci ili ako sudac izda nalog). Međutim, često će o tome odlučiti nadležno lokalno tijelo sukladno pravilima iz različitih primjenjivih instrumenata. SZP lokalne vlasti ima važnu ulogu u savjetovanju u odnosu na ovo pitanje (te se treba posavjetovati s nadležnim nadzornim tijelom ukoliko postoje bilo kakve dvojbe).

Na primjer, obrazovni odjel na lokalnoj razini može prikupljati osobne podatke o učenicima u obrazovne svrhe sukladno GDPR-u, međutim lokalna policija može zatražiti pristup (nekim od) tih podataka u svrhu rješavanja kriminala na lokalnoj razini (npr. kako bi provjerili koji učenici su određenog dana bili odsutni s nastave). Predložena obrada podataka za drugu svrhu bila bi u nadležnosti LED-a (ili preciznije rečeno, nacionalnog zakona u koji su prenesene odredbe LED-a, kao i pod nadležnošću određenih zakona odnosnih na policijske i kaznene postupke). Ponekad, primjenjivi zakoni ili zakonska pravila pojašnjavaju kada se takvi uvidi mogu izvršiti (npr. samo u vezi određenih zločina ili ukoliko postoji opravdana sumnja prema određenoj djeci ili ako sudac izda nalog). Međutim, često će o tome odlučiti nadležno lokalno tijelo sukladno pravilima iz različitih primjenjivih instrumenata. SZP lokalne vlasti ima važnu ulogu u savjetovanju u odnosu na ovo pitanje (te se treba posavjetovati s nadležnim nadzornim tijelom ukoliko postoje bilo kakve dvojbe). Na primjer, obrazovni odjel na lokalnoj razini može prikupljati osobne podatke o učenicima u obrazovne svrhe sukladno GDPR-u, međutim lokalna policija može zatražiti pristup (nekim od) tih podataka u svrhu rješavanja kriminala na lokalnoj razini (npr. kako bi provjerili koji učenici su određenog dana bili odsutni s nastave). Predložena obrada podataka za drugu svrhu bila bi u nadležnosti LED-a (ili preciznije rečeno, nacionalnog zakona u koji su prenesene odredbe LED-a, kao i pod nadležnošću određenih zakona odnosnih na policijske i kaznene postupke). Ponekad, primjenjivi zakoni ili zakonska pravila pojašnjavaju kada se takvi uvidi mogu izvršiti (npr. samo u vezi određenih zločina ili ukoliko postoji opravdana sumnja prema određenoj djeci ili ako sudac izda nalog). Međutim, često će o tome odlučiti nadležno lokalno tijelo sukladno pravilima iz različitih primjenjivih instrumenata. SZP lokalne vlasti ima važnu ulogu u savjetovanju u odnosu na ovo pitanje (te se treba posavjetovati s nadležnim nadzornim tijelom ukoliko postoje bilo kakve dvojbe). Uredba 2018/1725 daje određene smjernice o prijenosu osobnih podataka od strane institucija i tijela EU "primateljima s poslovnim nastanom u

203 Usp. članak 74. Uredbe 2018/1725 o "distinkciji između operativnih osobnih podataka i provjere kvalitete operativnih osobnih podataka", što je dobar primjer toga što bi trebala biti dobra opća praksa kada voditelj obrade sudjeluje u aktivnostima koje podliježu različitim režimima zaštite podataka.[205] Vidi Treći dio ovog priručnika.

204 Vidi Treći dio ovog priručnika.

205 Napominjemo kako je navedeni prijenos podataka drugačiji od prijenosa osobnih podataka jednog tijela drugom na području iste zemlje ili drugoj državi članici za istu svrhu, sukladno istom [EU] režimu zaštite podataka – npr. od strane jedne agencije za provođenje zakona u određenoj državi članici drugoj istovjetnoj agenciji u istoj državi ili u drugoj državi članici; te od prijenosa osobnih podataka u treće zemlje (za koje vrijede posebna pravila u odnosu na takvu vrstu transfera – uz napomenu da i u tom slučaju postoje određene režimske razlike).

Uniji, a koji nisu institucije ili tijela Unije" – uglavnom su to javna tijela država članica. Institucijama i tijelima EU dopušteno je vršenje prijenosa podataka tijelima država članica, uz uvjet da:

(a) primatelj [tj. tijelo u državi članici koje zahtijeva podatke] dokaže kako su podaci nužni za izvršenje zadaća koje su od javnog interesa ili za izvršenje službenih ovlasti primatelja [tj. tijela]; ili

(b) primatelj dokaže da je prijenos podataka potreban za određenu svrhu koja je u javnom interesu i da voditelj obrade [tj. institucija ili tijelo EU od kojeg je zatražena dostava podataka] gdje postoji bilo kakav razlog za sumnju da se legitimni interesi ispitanika dovode u pitanje, utvrdi da je razmjerno prenošenje osobnih podataka za tu određenu svrhu, nakon što je odmjerio različite interese (čl. 9(1)).

Institucijama ili tijelima EU dopušten je prijenos (slanje) takvih podataka tijelima u državama članicama bez zahtijevanja, tj. temeljem vlastitog prijedloga, ukoliko mogu:

> dokazati da je prijenos osobnih podataka nužan i razmjeran svrhama prijenosa primjenom kriterija navedenih u točkama (a) i (b) iz stavka 1. (čl. 9(2)).

Međutim, u tom slučaju potrebno je uzeti u obzir nekoliko stvari. Prvenstveno, navedeno se odnosi na institucije i tijela EU koja nisu uključena u policijsku i pravosudnu suradnju, tj. primjenjuje se samo na obradu – i prijenos – u odnosu na "glavni režim" temeljen na Uredbi 2018/1725 za institucije i tijela EU; i kako je navedeno u odlomku 1.4.5. iznad, da je "glavni" režim zaštite podataka u toj uredbi usklađen s GDPR-om. Ne postoji odgovarajuća odredba o prijenosu osobnih podataka tijelima u državama članicama u Poglavlju IX Uredbe 2018/1725, koja obuhvaća obradu "operativnih" osobnih podataka od strane institucija i tijela EU koja su uključena u policijsku i pravosudnu suradnju.

Nadalje, prethodno istaknuta pravila iz članka 9 "ne dovode u pitanje" temeljna načela zaštite podataka, uključujući ograničavanje svrhe i pravilo o "usklađenoj" obradi (vidi čl. 6 Uredbe koji navodi značajne uvjete), relevantnost podataka itd. kao ni odredbe o zakonitosti obrade (vidi uvodnu klauzulu članka 9(1)). Također, predmetna pravila ne dovode u pitanje ni posebna pravila obrade osjetljivih osobnih podataka (*idem).*

Ipak, članak 9. Uredbe 2018/1725 navodi da, **kada se osobni podaci obrađuju u skladu s jednim od prethodno navedenih režima, moraju se prenijeti drugom tijelu (ili čak koristiti od strane istog tijela) za obradu sukladno drugom režimu, uz odgovore na važna pitanja o svrsi, relevantnosti i primjerenosti podataka te o zakonitosti nužnosti i razmjernosti promjene svrhe.**

S tim u vezi, važno je zapamtiti, prije svega da "prijenos" podataka, kao i svaki drugi oblik "otkrivanja" osobnih podataka (uključujući činjenje osobnih podataka dostupnima, npr. na internetu) podrazumijeva oblik obrade (vidi čl. 4(2) GDPR-a, doslovce ponovljeno u svim drugim instrumentima zaštite podataka EU). Također, važno je da svaki "prijenos" osobnih podataka između različitih tijela uvijek ima dva aspekta:

- za subjekt koji šalje podatke, to je način objavljivanja podataka (vidi iznad); ali
- za primatelja to predstavlja prikupljanje osobnih podataka – što je zasebna aktivnost obuhvaćena općim konceptom "obrade", različitim od "otkrivanja", "prijenosa" ili "činjenja dostupnim" osobnih podataka.

Ako su, u odnosu na svoje odgovarajuće aktivnosti u vezi s prijenosom podataka, dva tijela subjekti različitih režima zaštite podataka, svaki od njih treba procijeniti usklađenost svog djelovanja s pravilima zaštite podataka primjenjivim na navedeno.

Dakle, u gornjem primjeru, lokalni odjel za obrazovanje podliježe GDPR-u i svim „budućim posebnostima" primjene odredbi GDPR-a kroz odgovarajuće nacionalne propise o zaštiti podataka (ili možda odgovarajućim dijelovima propisa o zaštiti podataka, vezanih za zadaće i ovlasti lokalnog odjela za obrazovanje, koji bi također trebali biti u skladu s GDPR-om).

S druge strane, lokalna policijska agencija podliježe nacionalnim pravnim propisima usvojenim u svrhu provedbe LED-a (kao i svim odgovarajućim pravilima iz nacionalnih policijsko ili kaznenopravnih postupaka, koje također trebaju biti u skladu s LED-om). U tom slučaju, lokalni odjel za obrazovanje mora izvršiti provjeru (uz pomoć njegovog SZP-a i po potrebi savjetovati se s nadležnim tijelom za zaštitu podataka) dopuštaju li pravila o zaštiti podataka kojima isti podliježe, otkrivanje osobnih podataka policijskoj agenciji/policiji (ili ne, ili pod kojim uvjetima).

Suprotno tome, lokalna policija/policijska agencija trebala bi, prije podnošenja zahtjeva za dostavu podataka odjelu za obrazovanje, provjeriti (uz pomoć svog SZP-a i po potrebi kroz savjetovanje s nadležnim tijelom za zaštitu podataka) dopuštaju li mu pravila kojima podliježe da zatraži osobne podatke od lokalnog tijela za obrazovanje (ili ne, ili pod kojim uvjetima).

Često će biti korisna komunikacija dvaju SZP-a o predmetnom problemu (te zajedničko konzultiranje s nadležnim tijelom za zaštitu podataka gdje je to primjereno).

Često su određena pravila međusobno kompatibilna te upućuju jedna na druga. Primjerice, policijski zakon može predviđati kada i pod kojim uvjetima, lokalna policijska agencija može zatražiti "druga javna tijela" informaciju (općenito i/ili o djeci); a pravila koja se odnose na odjel za obrazovanje mogu propisivati da odjel može – ili mora – pružiti informacije koje je zatražilo neko "drugo javno tijelo/tijelo javne vlasti" (ili u predmetnom slučaju, policija), pod uvjetom da je zahtjev u skladu sa zakonom. Navedeno bi još uvijek zahtijevalo od policijske agencije da poštuje pravila i ispunjava određene uvjete, a od odjela za obrazovanje da barem zatraži jamstvo (ili dokaz) da je zahtjev policije zakonit i da ispunjava određene uvjete. Međutim, ako stavimo na stranu ta pitanja, ne postoji zapreka za prijenos podataka.

Kada su obje agencije, i ona koja vrši prijenos podataka kao i ona koja zahtijeva prijenos, predmet prethodno opisanih EU propisa o zaštiti podataka – posebno GDPR-a, LED-a i Uredbe 2018/1725 – u pravilu ne postoje zapreke u tom pogledu (iako pojedinačni slučajevi još uvijek mogu zahtijevati ozbiljnu analizu i pažnju).

Pitanja su manje jasna kada tijelo – u pravilu ono koje šalje zahtjev – nije predmet/subjekt posljednjih propisa/pravila, već samo manje zahtjevnih naslijeđenih pravila – iako su i ta pravila temeljena na općim načelima zaštite podataka na kojem se temelje svi EU propisi o zaštiti podataka.

Međutim, u praksi se stvari mogu ozbiljno zakomplicirati kada tijelo koje podnosi zahtjev, uopće nije subjekt nikakvog odgovarajućeg propisa o zaštiti podataka – kao što je slučaj, kako smo vidjeli, u odnosu na pitanja ZVSP-a, pitanja odnosna na EU očuvanje mira ili druge vojne misije ili nacionalna sigurnost. U ovom kontekstu, "odgovarajuća" pravila su pravila koja se jasno temelje i priznaju načela opće zaštite podataka; koja odstupaju od uobičajenih pravila izgrađenih na navedenim načelima samo u onoj mjeri u kojoj je to posebno određeno (javno dostupnim, jasnim i preciznim) pravnim instrumentom koji "je predvidljiv" u svojoj primjeni i samo u onoj mjeri u kojoj je "strogo nužno" za ispunjenje određene svrhe, s tim da je navedeno "razmjerno" posebnom kontekstu;[206] i koja osiguravaju kontrolu primjene posebnih pravila od strane neovisnog tijela.[207]

206 To su zahtjevi vladavine prava koje je razvio Europski sud za ljudska prava i jednako ih primjenjuje Sud EU te se odražavaju i u EU Povelji o temeljnim pravima (PTP), a kojih se mora pridržavati svaka demokratska država u svom djelovanju koje može imati utjecaja na temeljna prava i slobode pojedinca. [208] Kao što je izričito predviđeno u čl. 8(3) PTP-a.

207 Kao što je izričito predviđeno u čl. 8(3) CFR-a.

Ovo nije mjesto za detaljniju raspravu o navedenom. Međutim, nekakvo šire viđenje se može postaviti.

Dakle, svaki prijenos osobnih podataka od strane nacionalnog tijela javne vlasti (ili institucija ili tijela EU) koji podliježu zadnjim EU propisima o zaštiti podataka (tj. GDPR-a, LED-a ili Uredbe 2018/1725) bilo kojem nacionalnom ili EU tijelu koje uopće ne podliježe odgovarajućem propisu o zaštiti podataka, potencijalno narušava EU zaštitu podataka kao bilo koji takav prijenos u zemlje koje nemaju odgovarajuće propise o zaštiti podataka – što je u osnovi zabranjeno, osim ukoliko su usvojene "odgovarajuće zaštitne mjere" (usp. poglavlje V GDPR-a).

Tijela koja podliježu nekom od prethodno spomenutih EU instrumenata zaštite podataka, trebala bi biti na oprezu prije pružanja osobnih podataka koje obrađuju temeljem navedenih instrumenata, tijelima koja potražuju te podatke, a ne podliježu ni jednom odgovarajućem propisu o zaštiti podataka. Trebala bi uvijek pažljivo provjeriti – kao i uvijek, uz pomoć svog SZP-a i po potrebi konzultirati nadležno tijelo za zaštitu podataka – dopušta li instrument kojem oni podliježu takav oblik prijenosa (uopće) ili zabranjuje ili postavlja određene uvjete; te bi trebali odbiti izvršiti prijenos podataka, osim ukoliko nije dopušten u odnosu na određeni instrument, pod dovoljno jasnim uvjetima.

Nije dovoljno za tijelo koje podnosi zahtjev, a ne podliježe odgovarajućim propisima zaštite podataka, da samo ukaže tijelu od kojeg traži podatke kako mu je dopušteno prikupljanje podataka koje traži sukladno pravilima koja se primjenjuju na to tijelo: navedeno može ozakoniti prikupljanje podataka u skladu s tim pravilima, ali ne može ozakoniti otkrivanje podataka (prijenos) od strane tijela koje podliježe propisima o zaštiti podataka (posebice ukoliko su ta pravila postavljena sukladno prethodno navedenim posljednjim EU instrumentima zaštite podataka).

Ponekad države još uvijek imaju na snazi pojedine zakone koji daju njihovim agencijama – u pravilu, njihovim obavještajnim agencijama – pravo da zahtijevaju informacije ili pristup informacijama, uključujući osobne podatke u najširem smislu; te su ponekad zakoni postavljeni na način da nadjačaju bilo kakva ograničenja u otkrivanju osobnih podataka od strane tijela koja podliježu zakonima o zaštiti podataka i koja se (kako to široko postavljaju zakoni) moraju uskladiti s takvim zahtjevima, bez obzira na to što određeni propisi o zaštiti podataka kojima isti podliježu propisuju. To uključuje zakone u državama članicama.[208]

Što se tiče nacionalnih sigurnosnih agencija, država članica može tvrditi da propisi koji se odnose na takve agencije mogu zahtijevati informacije (ili pristup bazama podataka) koji se nalaze izvan opsega EU zakona – te da je prijenos podataka takvim agencijama sukladno njihovim propisima također izvan opsega EU zakona i izvan ovlasti tijela nadležnih za zaštitu podataka ili Suda EU.

Međutim, to bi bilo pogrešno tumačenje pravnih postavki. Čak i ako je prikupljanje osobnih informacija od strane takvih agencija izvan opsega EU zakona (ili ovlasti nadležnih tijela za zaštitu podataka i Suda EU), prijenos podataka takvim agencijama od strane bilo kojeg tijela koje podliježe EU instrumentima zaštite podataka, podliježe EU zakonu. Voditelji obrade takvih tijela i njihovi SZP-ovi trebaju biti svjesni toga i konzultirati se s nadležnim tijelima za zaštitu podataka kada god se pojavi takav slučaj.

1.4.7. "Modernizirana" Konvencija Vijeća Europe za zaštitu podataka iz 2018.

Premda je Konvencija Vijeća Europe iz 1981. g. donesena (široko) u skladu s Direktivom o zaštiti podataka EZ-a iz 1995. g., dodavanjem pravila o prekograničnom protokolu podataka i o neovisnim tijelima za zaštitu podataka u svojem Dodatnom protokolu, usvojenom 2001. g. (kako je opisano pod točkom 1.3.2, prethodno u tekstu), ona je i dalje, kao i ta Direktiva, postala zastarjela do kraja prvog desetljeća 21. stoljeća. Rad na "moderniziranju" Konvencije započeo je 2011. godine, te je "modernizirana Konvencija" usvojena i ot-

208 Douwe Korff *et al, Granice prava* (bilješka 172, iznad), Dio 4.

vorena za potpisivanje 18. svibnja 2018. g.[209] U vrijeme pisanja ovog priručnika, ona još nije stupila na snagu: to će se dogoditi tri mjeseca nakon što pet država članica Vijeća Europe pristupi Moderniziranoj Konvenciji (čl. 26(2)) – ali, naravno, čak i tada samo u odnosu na one države članice, stranke Konvencije iz 1981. g. (te, gdje je to primjenjivo, njenog Dodatnog protokola), nastavit će se primjenjivati stara Konvencija (i njen Protokol).[210]

Samo Vijeće Europe izradilo je vrlo koristan **pregled novosti u moderniziranoj Konvenciji**, što je izloženo u nastavku:[211]

Glavne novosti[212] modernizirane Konvencije mogu se prikazati kako slijedi:

CILJ I SVRHA KONVENCIJE (ČLANAK 1.)

Prema članku 1., cilj Konvencije jasno je naglašen, a to je - konkretno jamčiti svakom pojedincu unutar nadležnosti neke od država stranaka (neovisno o njihovom državljanstvu ili mjestu boravišta) zaštitu njihovih osobnih podataka koji se obrađuju, time doprinoseći poštivanju njihovih prava i temeljnih sloboda, a posebice njihovog prava na privatnost.

Koristeći ovu terminologiju, Konvencija naglašava činjenicu da obrada osobnih podataka može pozitivno omogućiti ostvarivanje drugih temeljnih prava i sloboda, što se tako može olakšati jamčenjem prava na zaštitu podataka.

DEFINICIJE I PODRUČJE PRIMJENE (ČLANCI 2. I 3.)

Dok ključni pojmovi, kao što su definicija osobnih podataka ispitanika, nisu uopće modificirani,[213] druge promjene predložene su u definicijama: koncept 'zbirke' je napušten. "Voditelj zbirke podataka" zamijenjen je terminom "voditelj obrade podataka", uz kojeg se koriste termini "izvršitelj" i "primatelj".

Područje primjene uključuje i automatiziranu i neautomatiziranu obradu osobnih podataka (ručna obrada, kada podaci tvore dio strukture koja omogućava pretraživanje subjekta podataka prema unaprijed određenim kriterijima) što potpada pod nadležnost stranke Konvencije. Sveobuhvatna priroda Konvencije je očuvana, a područje primjene se prirodno nastavlja kako bi obuhvatilo obradu i u javnom i u privatnom sektoru, jer je to jedna od doista jačih strana Konvencije.

S druge strane, Konvencija se više ne primjenjuje na obradu podataka koju fizičke osobe obavljaju u okviru isključivo osobne ili kućne aktivnosti.[214]

Nadalje, ugovorne strane više nemaju mogućnost dati izjave usmjerene na izuzimanje određenih vrsta obrade podataka od primjene Konvencije (npr. nacionalna sigurnost i obrana).

OBVEZE STRANAKA (ČLANAK 4.)

Svaka stranka u svojem nacionalnom pravu mora provesti mjere potrebne da bi se pokazao učinak

209 Vidjeti: https://www.coe.int/en/web/data-protection/background-modernisation "Modernizirana konvencija" bila je uglavnom spremna do 2014., ali je njezino formalno otvaranje za potpisivanje bilo odgođeno, djelomično kako bi se omogućila usklađenost s BDPR-om, a dijelom kako bi se riješile zabrinutosti jedne velike države članice Vijeća Europe. Protokol o izmjenama i dopunama Konvencije o zaštiti pojedinaca s obzirom na automatsku obradu osobnih podataka, CETS 223, dostupan je na: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223 Pročišćeni tekst Modernizirane konvencije dostupan je na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

210 Do sredine prosinca 2018. godine, 22 države su potpisale Moderniziranu konvenciju, ali je još nisu ratificirale. Vidjeti: https://www.coe.int/en/web/conventions/search-on-treaties/- /conventions/treaty/223/signatures?p_auth=ZmXAeCCF Posebni izvjestitelj UN-a za pravo na privatnost preporučio je svjetsku ratifikaciju "Modernizirane" Konvencije od 2018.

211 Preuzeto sa: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8 Sve pojedinosti o specifičnim tekstualnim promjenama u obliku komparativne tabele dostupne su ovdje: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958

212 Ovaj pregled iznosi novosti i ne ponavlja odredbe koje postoje već od Konvencije iz 1981.g. i njenog dodatnog Protokola iz 2001.g. Za cjeloviti pregled modernizirane Konvencije, molimo pročitajte pročišćenu verziju objavljenu na internetskim stranicama Vijeća Europe.

213 Ali važno je primijetiti da je dodano prilično "ulašteno" Obrazloženje (*Explanatory Memorandum*) uz moderniziranu Konvenciju (dodana bilješka (fusnota)).

214 Takva "isključivo osobna obrada" prvo je isključena iz pravila o zaštiti podataka u Direktivi o zaštiti podataka iz 1995. g., kako bi se osiguralo poštivanje prava na privatni život; to je ponovljeno u GDPR-u (dodana bilješka (fusnota)).

odredbi Konvencije.

Nadalje, svaka ugovorna stranka treba dokazati da su takve mjere doista i poduzete te da su na snazi i prihvaćaju da Odbor za konvenciju može provjeriti je li ovim zahtjevima udovoljeno. Ovaj [*novi*] proces procjene ugovornih stranaka ("mehanizam daljnjeg praćenja") nužan je kako bi se jamčilo da su države stranke doista i ostvarile ovaj stupanj zaštite ustanovljen Konvencijom.

Važno je primijetiti da međunarodne organizacije sada imaju mogućnost pristupiti Konvenciji (članak 27), kao i Europska unija (članak 26).

ZAKONITOST OBRADE PODATAKA I KVALITETA PODATAKA (ČLANAK 5.)

Članak 5. pojašnjava primjenu načela proporcionalnosti kako bi naglasio da se ono mora primjenjivati kroz čitavu obradu, a posebice u pogledu sredstava i metoda korištenih kod obrade. Nadalje, to je još više naglašeno načelom minimizacije podataka.

Uvedena je nova odredba kako se jasno propisala pravna osnova obrade: privola (koja mora udovoljavati nekoliko kriterija da bi bila valjana) ispitanika ili neka druga zakonita osnova propisana zakonom (ugovor, vitalni interesi subjekta podataka, pravna obveza voditelja obrade itd.).

OSJETLJIVI PODACI (ČLANAK 6.)

Katalog osjetljivih podataka proširen je kako bi uključio genetske i biometrijske podatke (koji su utjecali na EU), kao i podatke obrađene radi informacija koje otkrivaju, a odnose se na članstvo u sindikatu ili nacionalno podrijetlo (ove posljednje dvije kategorije dodane su postojećoj [*načelnoj*] zabrani obrade osobnih podataka kojima se otkriva rasno podrijetlo, politička mišljenja ili religijska, te ostala uvjerenja, zdravstveni podaci ili podaci o seksualnom životu te osobni podaci koji se odnose na kaznena djela, kaznene postupke i kaznene osude).

SIGURNOST PODATAKA (ČLANAK 7.)

U smislu sigurnosti podataka, uveden je zahtjev obavijestiti, bez odugovlačenja, o bilo kojim povredama sigurnosti. Ovaj je zahtjev ograničen na slučajeve koji mogu ozbiljno narušiti prava i temeljne slobode ispitanika, a treba ih se prijaviti barem nadzornim tijelima.

TRANSPARENTNOST OBRADE (ČLANAK 8.)

Voditelji obrade imaju obvezu jamčiti transparentnost obrade podataka i radi toga moraju osigurati traženi set informacija, posebno u odnosu na njihov identitet i uobičajeno boravište ili poslovni nastan, o pravnim osnovama i svrhama obrade, primateljima podataka i kategorijama obrađivanih osobnih podataka. Trebali bi nadalje osigurati bilo koje dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada. Voditelj obrade je izuzet od pružanja takvih informacija kada je obrada izrijekom propisana zakonom ili se to pokaže nemogućim ili pak uključuje nerazmjerne napore.

PRAVA ISPITANIKA (ČLANAK 9.)

Ispitanici imaju nova prava tako da imaju veću kontrolu nad svojim podacima u ovo digitalno doba.

Modernizirana Konvencija proširuje katalog informacija koje se trebaju poslati ispitanicima kad oni ostvaruju svoje pravo pristupa svojim osobnim podacima. Nadalje, ispitanici imaju pravo saznati koja je logika u podlozi obrade podataka, rezultati čega se primjenjuju na nju ili njega. Ovo novo pravo je

posebice važno u smislu profiliranja pojedinaca.[215]

Ovo se povezuje s još jednom novosti, naime pravom ne biti podvrgnut odluci koja utječe na ispitanika, a koja se temelji isključivo na automatiziranoj obradi, bez da se uzimaju u obzir mišljenja ispitanika.

Ispitanici imaju pravo prigovoriti u bilo koje doba tome da se njihovi podaci obrađuju, osim ako voditelj obrade dokaže nedvojbene legitimne osnove za obradu, koji su pretežniji od njihovih interesa ili prava i temeljnih sloboda.

DODATNE OBVEZE (ČLANAK 10.)

Modernizirana Konvencija nameće opširnije obveze onima koji obrađuju podatke ili na čiji se zahtjev podaci obrađuju.

Odgovornost postaje integralan dio sheme zaštite, s obvezom voditelja obrade da budu u mogućnosti dokazati usklađenost s pravilima o zaštiti podataka.

Voditelji obrade trebaju poduzeti sve odgovarajuće mjere – uključujući i kad je obrada povjerena trećoj strani – kako bi jamčili da je pravo na zaštitu podataka osigurano (tehnička zaštita podataka, ispitivanje vjerojatnog učinka namjeravane obrade podataka na prava i temeljne slobode subjekata podataka ("procjena učinka na privatnost") i integrirana zaštita podataka).

IZNIMKE I OGRANIČENJA (ČLANAK 11.)

Prava propisana Konvencijom nisu apsolutna i mogu biti ograničena kada je to propisano zakonom i kada predstavlja nužnu mjeru u demokratskom društvu na temelju određenih i ograničenih osnova. Među tim ograničenim osnovama sada su uključeni "bitni ciljevi javnog interesa", kao i pozivanje na pravo slobode izražavanja.

Popis odredbi Konvencije koje se mogu ograničiti blago je proširena (vidjeti reference na članke 7.1 o sigurnosti i 8.1 o transparentnosti u članku 11.1), a novi stavak ovog članka posebice se bavi aktivnostima obrade za svrhe nacionalne sigurnosti i obrane, za koje se mogu ograničiti neke "nadzorne" ovlasti Odbora, kao i neke zadaće nadzornih tijela. Zahtjev da postupci obrade u svrhe nacionalne sigurnosti i obrane budu podložni neovisnom i učinkovitom pregledu i nadzoru jasno je predviđen.

Važno je prisjetiti se još jednom da, suprotno ranijim odredbama Konvencije 108, ugovorne stranke modernizirane Konvencije više neće moći isključiti određene vrste obrade iz opsega primjene Konvencije.

PREKOGRANIČNI PROTOK OSOBNIH PODATAKA (ČLANAK 14.)[216]

Cilj ove odredbe je olakšati, kada je to moguće, slobodan protok informacija, neovisno o granicama, istodobno osiguravajući odgovarajuću zaštitu pojedincima u pogledu obrade osobnih podataka.

U odsustvu usklađenih pravila o zaštiti koje bi dijelile države koje pripadaju regionalnim međunarodnim organizacijama i pravila koja su mjerodavna za prekogranični protok (vidjeti primjerice okvir zaštite podataka Europske unije), protok podataka između stranaka bi stoga trebao funkcionirati slobodno.

U pogledu prekograničnog potoka podataka primatelju koji nije podložan nadležnosti države stranke treba biti jamčena, odgovarajuća razina zaštite u državi primateljici ili organizaciji. Kako se ovo ne može presumi-

215 O ovoj temi, vidjeti preporuku Recommendation (2010) 13 on the Protection of Individuals with regard to Automatic Processing of Personal Data in the context of profiling i njeno Obrazloženje (Explanatory memorandum) (izvorna bilješka (fusnota)).
216 U tom smislu, modernizirana Konvencija nadograđuje se na Dodatni protokol i EU pravila.

rati jer primateljica nije ugovorna stranka, Konvencija ustanovljuje dva glavna sredstva kako bi se osiguralo da razina zaštite doista bude odgovarajuća; bilo zakonom, ili *ad hoc* ili odobrenim standardiziranim zaštitnim mjerama koje su zakonski obvezujuće i provedive (posebice ugovornim odredbama ili obvezujućim korporativnim pravilima), kao i da su valjano provedene.

NADZORNA TIJELA (ČLANAK 15.)

Temeljeći se na članku 1. Dodatnog protokola, modernizirana Konvencija nadopunjuje katalog ovlasti tijela odredbama da, pored njihovih ovlasti intervenirati, istražiti, uključiti se u sudske postupke ili skrenuti pažnju sudskim tijelima na povrede odredbi o zaštiti podataka, tijela također imaju obvezu podizati svijest, pružati informacije i educirati sve uključene stranke (ispitanike, voditelje obrade, izvršitelje itd.). Također dopušta tijelima da donesu odluke i nametnu sankcije. Nadalje, navodi se da bi nadzorna tijela trebala biti neovisna prilikom ostvarenja ovih svojih zadaća i ovlasti.

OBLICI SURADNJE (ČLANAK 17.)

Modernizirana Konvencija također se dotiče pitanja suradnje (i međusobne pomoći) između nadzornih tijela.

Nadzorna tijela moraju koordinirati svoje istrage, provoditi zajedničke nadzore i osigurati jedna drugima relevantne informacije i dokumentaciju o svojem pravu i upravnim praksama koje se odnose na zaštitu podataka.

Informacije razmijenjene između nadzornih tijela uključivat će osobne podatke samo kada su takvi podaci neophodni za suradnju ili kada je ispitanik dao posebnu, dobrovoljnu i informiranu privolu.

Konačno, Konvencija predviđa forum za povećanu suradnju: nadzorna tijela država stranaka moraju stvoriti mrežu kako bi organizirala svoju suradnju i provela svoje zadaće kako je to navedeno u Konvenciji.

ODBOR ZA KONVENCIJU (ČLANCI 22., 23. I 24.)

Odbor za Konvenciju igra ključnu ulogu u tumačenju Konvencije, poticanju razmjene informacija između država članica i razvoju standarda zaštite podataka.

Uloge i ovlasti ovog Odbora ojačane su moderniziranom Konvencijom. To više nije ograničeno samo na "savjetodavnu" ulogu, već Odbor sada ima i ovlasti procjene i nadzora. [*Osim davanja*] mišljenja o razini zaštite podataka koju pruža neka država [*kao i ranije, sada će to također činiti i u pogledu*] međunarodne[ih] organizacije[*a*] prije pristupanja Konvenciji. Odbor je [*sada*] također u mogućnosti procijeniti usklađenost domaćeg nacionalnog prava dotične stranke i odrediti učinkovitost poduzetih mjera (postojanje nadzornog tijela, odgovornosti, postojanje učinkovitih pravnih lijekova).

Također je u mogućnosti procijeniti pružaju li pravne norme mjerodavne za prijenos podataka dostatna jamstva odgovarajuće razine zaštite podataka.

Ovo nije pravo mjesto za detaljnu analizu ovih novosti. Dostatno je primijetiti da **ove novosti donose nov, "moderniziran" režim Konvencije blizak novom režimu ustanovljenom za EU temeljem GDPR-a**. To znači da kada će EU procijeniti "dostatnost" režima zaštite podataka u trećoj državi (kako je izloženo u Drugom dijelu, pod točkom 2.1), činjenica da treća država jest stranka modernizirane Konvencije bila bi glavno pitanje koje treba razmotriti.

Doista, u okviru **polja primjene**, modernizirana Konvencija nadilazi GDPR, jer vrlo jasno izražava i u tekstu modernizirane Konvencije, a i u gornjem pregledu, da države stranke modernizirane Konvencije više neće moći isključiti bilo koje vrste obrade iz svojih obveza – kao što su ***nacionalna sigurnost*** i ***obrana***, što su pitanja izvan polja primjene EU instrumenata za zaštitu podataka.[217]

Pitanje hoće li u drugom smislu modernizirana Konvencija – ili preciznije rečeno, nacionalni zakoni država članica modernizirane Konvencije koje primjenjuju tu Konvenciju – biti uvijek u cijelosti u skladu s GDPR-om - ili preciznije, s GDPR-om kako će ga u budućnosti tumačiti i primjenjivati novi Europski odbor za zaštitu podataka, tijela za zaštitu podataka iz EU država članica, Europske Komisije i SEU-a – to je pitanje na koje odgovor naravno tek predstoji.

Primjerice, nova pravila o prekograničnom protoku podataka u moderniziranoj Konvenciji dopuštaju prijenos u treće zemlje koje osiguravaju "***odgovarajuću***" razinu zaštite (čl. 14) – što se naizgled može činiti sličnim zahtjevu "***primjerene***" razine zaštite u GDPR-u (kao i prema Direktivi o zaštiti podataka iz 1995. g.) ostaje za vidjeti kako će novi Odbor za Konvenciju slijediti SEU u njegovom stavu da ovaj izraz "odgovarajuća" treba biti tumačen kao da znači da treća država o kojoj se radi mora osigurati "***u bitnome ekvivalentnu***" zaštitu (kako je SEU presudio u tumačenju izraza "odgovarajuća").[218]

U drugim vidovima, primjerice, što se tiče **privole djece**, modernizirana Konvencija nije toliko detaljna ni podrobna kao odredbe iz GDPR-a.

Ali ako stavimo ova pitanja sa strane, jasno je da Vijeće Europe i Europska unija vode prema ustanovljavanju globalnih "zlatnih standarda" za zaštitu podataka, i u pogledu primjene unutar država, ali također i u pogledu prekograničnih protoka podataka.

Na kraju, treba primijetiti da je modernizirana Konvencija (za razliku od prethodne) otvorena pristupanju međunarodnih organizacija – i stoga EU može formalno pristupiti istoj.

217 Vidjeti tekst u točki 1.3.1, prethodno u tekstu, pod naslovom "*Priroda i ograničenja EZ direktiva*", u pogledu ovog ograničenja u odnosu na EZ direktive o zaštiti podataka iz 1995. i 2002. g., kao i Drugi dio, pod točkom 2.1, dalje u tekstu, u pogledu GDPR-a. U odnosu na obradu u svrhe provedbe zakona (itd.), kao i obradu od strane samih EU institucija, EU naravno ima postojeća pravila, koja su u načelu sukladna standardima GDPR-a (i stoga i moderniziranoj Konvenciji) (ili u odnosu na EU institucije, to će učiniti kad one jednom budu usklađene s GDPR-om).

218 SEU, *Schrems* presuda (bilješka (a) 73, prethodno u tekstu), odlomak 73. presuda SEU-a u Slučaju C362/14, 6. prosinca 2015.

DRUGI DIO
Opća uredba o zaštiti podataka

2.1 UVOD

Kako je već prethodno navedeno u tekstu pod točkom 1.4.1, Opća uredba o zaštiti podataka (GDPR ili "Uredba") usvojena je dijelom zato što Direktiva o zaštiti podataka iz 1995. g. nije dovela do dostatne razine usklađenosti zakona država članica; dijelom kao odgovor na masivnu ekspanziju obrade osobnih podataka od uvođenja Direktive o zaštiti podataka iz 1995. g.; a dijelom kao odgovor na sudsku praksu SEU-a. Ostaje za vidjeti hoće li biti dostatna odgovoriti na razvoj sve intruzivnijih tehnologija, kao što su *the Big Data*, *the Internet of Things*, algoritamsko donošenje odluka i korištenje umjetne inteligencije.

Uredba se temelji na Direktivi o zaštiti podataka iz 1995. g., ali značajno je proširuje i, u tom nastojanju, značajno osnažiti glavni EU režim zaštite podataka. Ona donosi *veću harmonizaciju, snažnija prava ispitanika, bliskiju suradnju tijela za zaštitu podataka, snažnije ovlasti provedbe* i više od toga.

Prilog 1 uz ovaj priručnik sadrži *Kazalo (indeks) poglavlja, odjeljaka i članaka GDPR-a*, radi lakšeg snalaženja. Prilog 2 sadrži cjelovit tekst Uredbe, kako je objavljen u Službenom glasniku EU-a, uključujući i uvodne izjave.

Odjeljak 3.2 objašnjava status i pristup GDPR-a te detaljno raspravlja o implikacijama činjenice da sadrži mnoge klauzule koje dopuštaju daljnje reguliranje na nacionalnoj razini (čime se donekle ispunjava cilj potpunijeg usklađivanja).

Odjeljak 3.3 pruža pregled poglavlje po poglavlje, odjeljak po odjeljak i članak po članak.

Potom se okrećemo dvama ključnim pitanjima za SZP-ove: novo načelo "pouzdanosti" ["odgovornosti"] (obveza dokazivanja usklađenosti) (tekst u odlomku 2.4) i pravila o imenovanju, zahtjevima, uvjetima i zadaćama (itd.) SZP-a (tekst u odlomku 2.5), te objašnjenje povezanosti između ova dva.

2.2. PRAVNI POLOŽAJ I PRISTUP GDPR-A: IZRAVNA PRIMJENA UZ FLEKSIBILNOST

Uredba ...

GDPR je **uredba** – što znači: zakon EU-a koji je ***izravno primjenjiv*** u pravnim porecima država članica EU-a (i državama EGP-a koje nisu u EU), bez potrebe da bude "prenesena" u nacionalno zakonodavstvo, kao što je inače slučaj s direktivama, primjerice s Direktivnom o zaštiti podataka iz 1995. g.

EU zakonodavac je odabrao ovaj put upravo zato jer je provedba direktive iz 1995. g. bila neujednačena: bila je različito provedena u različitim državama članicama, što je dovelo do nepostojanja usklađenosti.[219]

Štoviše, bila je manjkavo primijenjena barem u nekima, kao primjerice u Ujedinjenom Kraljevstvu UK.[220]

U teoriji, uredba, koja je izravno primjenjiva, trebala bi dovesti do **pune usklađenosti** prava u području kojeg obuhvaća. U slučaju GDPR-a, ovo je još dodatno pojačano mnogo jačim dogovorima oko **dijeljenja informacija i suradnje** između zakonodavaca (nacionalna nadzorna tijela ili tijela za zaštitu podataka, TZP-ovi) i posebnim mehanizmom **"konzistentnosti"**, kako je objašnjeno u nastavku, pod tim naslovom.

Međutim, kako je prikazano pod sljedećim podnaslovom, GDPR u isto vrijeme i dalje ostavlja mnoga pitanja državama članicama EU da ih dalje reguliraju u nacionalnim zakonima, sukladno njihovim unutarnjim pravnim i institucionalnim uređenjima. Ovo bi moglo, u nekim područjima, potkopati cilj postizanja potpune usklađenosti, ali kako ćemo raspravljati pod naslovima "*Zahtjevi* posebnih klauzula" i "*Suradnja i konzistentnost*", također postoje granice slobode država članica u ovom pogledu, kao i nova sredstva nadzora na EU-razini, također i nad ostvarenjem tih "fleksibilnosti" (barem u teoriji).

… ali uz posebne klauzule[221]

Premda Uredba cilja ka većoj usklađenosti, ona i dalje sadrži brojne fleksibilne odredbe, koje je Komisija definirala kao "posebne klauzule" koje popuštaju u korist prava u državama članicama posebno u odnosu na javni sektor, ali također i u odnosu na obveze nametnute nacionalnim pravom društvima koja podliježu nadležnosti odnosne države članice (npr. prema radnom pravu ili pravilima o provedbi zakona).

VRSTE POSEBNIH KLAUZULA

Talijansko tijelo za zaštitu podataka, *Garante del Privacy*, identificiralo je četiri različite (iako donekle preklapajuće) vrste klauzula koje ostavljaju prostora za daljnju regulaciju pravom države članice:[222]

- **Daljnje specifikacije**

  Ovo su odredbe prema kojima države članice mogu zadržati ili uvesti "*preciznije odredbe kojima se prilagođava primjena*" relevantne odredbe ove Uredbe (koriste se različite fraze u tom smislu).

---

219 Ovo je već bio zaključak koji je iznijela studija koju je naručio EU, autora Douwe Korffa sa Sveučilišta u Essexu, Report on an EU study on the implementation of the [1995] data protection directive, 2002, dostupno na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 – ali je EU-u trebalo potom još 10 godina da se pozabavi ovim pitanjem predlažući donošenje uredbe.[221] Prema stavu EU Komisije, u 2011., gotovo trećina od 34 članka u Direktivi do tog doba nisu bila na pravi način primijenjena u UK-u, vidjeti: http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-dataprotection-act-is-deficient.html lako je Komisija prijetila poduzimanjem prisilne provedbe, to zapravo nije učinila, iako manjkavosti nikad nisu pravilno niti u cijelosti ispravljene.

220 Prema stavu EU Komisije, u 2011., gotovo trećina od 34 članaka u Direktivi do tog doba nije bilo primijenjeno na pravi način u UK-u, pogledati: http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-dataprotection-act-is-deficient.html lako je Komisija prijetila poduzimanjem prisilne provedbe, to zapravo nije učinila, iako manjkavosti nikad nisu pravilno niti u cijelosti ispravljene.

221 Vidi pododlomak "*Odnos između Direktive o e-privatnosti i GDPR-a", iznad.*

222 Antonio Caselli, prezentacija za prvi edukacijski sastanak "T4DATA", lipanj 2018, na temu "*GDPR i nacionalna pravila*". O sadržaju ove prezentacije izvještava se i razjašnjava unekoliko detaljno u Prilogu 4 uz priručnik (u Drugom svesku), gdje su također navedeni daljnji primjeri.

Primjeri:

Države članice mogu navesti koji postupci obrade zahtijevaju ***prethodno odobrenje***, ili regulirati korištenje ***nacionalnih identifikacijskih brojeva***, ili obradu ***osobnih podataka o zaposlenicima***.

Države članice mogu *„zadrža[ti] ili uv[esti]* ***dodatni[e] uvjet[e], uključujući ograničenja***, *u vezi s obradom* ***genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje"***, izvan ili preko uvjeta i ograničenja nametnutih samim GDPR-om u članku 9(1) – (3) (članak koji govori o „posebnim kategorijama osobnih podataka", koji se obično nazivaju „osjetljivi podaci") (čl. 9(4)). One mogu stoga, primjerice, propisati da je ***prethodna privola*** uvijek uvjet za obradu ***genetskih podataka***.

- **Opcije i izbori**

U nekim segmentima, GDPR dopušta državama članicama, putem njihovog nacionalnog prava, **odabrati** između nekih opcija posebno navedenih u Uredbi ili proširiti obvezu ili zabranu koja se prema GDPR-u primjenjuje samo u određenim slučajevima, na neke druge slučajeve.

Primjerice, države članice mogu dopustiti ***djeci*** starosti iznad 13, 14 ili 15 da ***daju privolu na određene informacijske usluge***, umjesto određenja da to bude dobna granica od 16 godina, kako je navedeno u GDPR-u; ili mogu tražiti ***imenovanje SZP-a*** u situacijama gdje GDPR to ne predviđa.

- **Ograničenja i odstupanja**

Uz primjenu određenih široko definiranih **uvjeta** (o čemu se raspravlja u nastavku, pod naslovima "*Zahtjevi posebnih klauzula*" i "*Problemi koje su izazvale* posebne klauzule) članak 23. GDPR-a omogućava **sveopća odstupanja** o zapravo svim pravima ispitanika u odnosu na široko definirane **važne ciljeve od općeg javnog interesa kao što su:** ***nacionalna sigurnost, obrana, javna sigurnost, provedba zakona*** i ***neovisnost pravosuđa*** – ali također i ***zaštite gospodarskih ili financijskih interesa države***, provedbe ***profesionalne etike***, bilo koje vrste "***praćenja, inspekcije ili regulatorne funkcije*** koja je, barem povremeno, povezana s izvršavanjem službene ovlasti" u bilo kojem od glavnih zaštićenih interesa, "***zaštita ispitanika ili prava i sloboda drugih***" i ***ostvarivanja potraživanja u građanskim sporovima***.

Članci 85., 86. i 89. GDPR-a svi sadrže odredbe koje, s druge strane, omogućuju (a u nekom smislu i zahtijevaju) **odstupanje** od određenih pravila iz GDPR-a kako bi se zaštitila **sloboda izražavanja**, omogućila **sloboda informiranja** (pristup dokumentima i informacijama koje vode javne vlasti) i **arhiviranje** te olakšalo (javni interes) **istraživanje**, dok se s druge strane nameću određeni **uvjeti** kod takvih odstupanja (što je također dalje raspravljeno pod naslovima "*Zahtjevi posebnih klauzula*" i "*Problemi koje su izazvale posebne klauzule*" dalje u tekstu).

Bilješka: neka od ovih posebnih pravila služe zaštiti interesa "drugih", dok se ostala mogu promatrati kao općenita ili od javnog interesa, a neka pak, kao sloboda informiranja, mogu poslužiti u oba slučaja. Ovo su pitanja u kojima pravila do sada nisu bila usklađena, iako u nekim državama članicama EU nadzor nad zaštitom podataka i nad slobodom informacija jesu stavljeni u nadležnost istih tijela. S obzirom da su takva pitanja sve više transnacionalna – tj. prekogranični zahtjevi za pristup javnim

podacima; sloboda izražavanja nasuprot problematike zaštite podataka i privatnosti vezano za internetske publikacije; transnacionalna medicinska istraživanja – može se očekivati da će EOZP izdati daljnje smjernice o tim pitanjima, posebno u odnosu na takve transnacionalne aktivnosti. Komisija bi također mogla predložiti nove inicijative u ovom području.

- Regu**latorne obv**eze

  U nekim situacijama, osim ovih prethodno navedenih – posebice u odnosu na ustanovljavanje neovisnih nadzornih tijela (tijela za zaštitu podataka, tzv. TZP-ovi), i ustanovljavanje mehanizama certificiranja – GDPR **zahtijeva** od država članica da usvoje detaljna pravila i propise, primjenjujući relevantne zahtjeve za TZP-ove u svojim nacionalnim pravnim porecima. Ovo su uglavnom tehnička pitanja (iako ona također zahtijevaju usklađenost s važnim standardima, npr. o neovisnosti i osiguravanju dostatnih resursa).

ZAHTJEVI POSEBNIH KLAUZULA

U mnogo aspekata, uključujući one spomenute pod naslovima "*daljnje specifikacije*" i "*opcije i izbori*", prethodno u tekstu, ali posebice one navedene pod naslovom "*ograničenja i odstupanja*", GDPR **traži** od država članica da usvoje **zakonska pravila** da se riješe relevantna pitanja ***koja udovoljavaju određenim demokratskim standardima/standardima ljudskih prava***.

Druge odredbe (koje nisu uključene pod ovim naslovima) također **impliciraju potrebu za regulacijom**, a u tome traže od država članica da usvoje "***prikladne zaštitne mjere***", "***odgovarajuće zaštitne mjere***" ili "***odgovarajuće mjere***". S obzirom da sam GDPR često ne objašnjava što bi ove zaštitne mjere ili mjere mogle biti, države članice će morati razjasniti to pitanje u svojim nacionalnim zakonima – koji će opet morati udovoljavati određenim demokratskim ***standardima/standardima*** vladavine prava.

Važno je zamijetiti da **u tom smislu, državama članicama nije jednostavno dodijeljeno neograničeno diskrecijsko pravo** – što jasno proizlazi iz zahtjeva da određene mjere ili zaštitne mjere trebaju biti "prikladne" ili "odgovarajuće". U drugim aspektima, određeni opće primjenjivi standardi i zahtjevi vladavine prava izrijekom su izraženi u GDPR-u – ali, u biti, slični standardi i zahtjevi primjenjuju se na svu relevantnu regulativu.

Stoga, GDPR izrijekom propisuje da načelno sveobuhvatna odstupanja dopuštena sukladno članku 23. (sažeto prethodno u tekstu pod naslovom "*Ograničenja i odstupanja*") moraju biti propisana u **zakonu** ("***zakonska mjera***") koji "***poštuje bit temeljnih prava i sloboda*** *te [] predstavlja* ***nužnu i razmjernu*** *mjeru u demokratskom društvu za zaštitu*" relevantnog interesa. Ovi zahtjevi su izravni odraz zahtjeva koji moraju biti zadovoljeni kod bilo kojeg ograničenja bilo kojeg od glavnih prava zaštićenih Europskom konvencijom za zaštitu ljudskih prava (EKLJP) i Povelja Europske unije o temeljnim pravima (PTP). Citirajmo potonju:

> Svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su **potrebna** i ako **zaista odgovaraju ciljevima od općeg interesa** koje priznaje Unija ili **potrebi zaštite prava i sloboda drugih osoba** (čl. 52(1), dodatno naglašeno).

S obzirom da svaki zakon države članice, koji ograničava bilo koja prava ispitanika sukladno bilo kojim posebnim klauzulama iz GDPR-a, suštinski predstavlja ograničenje prava na zaštitu podataka zajamčeno u Povelji (članak **8), svi takvi zakoni moraju udovoljavati gore navedenim standardima.**

Točnije, sukladno EKLJP-u i PTP-u, a time također i GDPR-u, relevantan zakon mora udovoljavati određenim bitnim **"kvalitativnim" zahtjevima**: pravila u zakonu moraju biti "**u skladu s vladavinom prava**" (što pose-

bice znači da ne smiju biti ***diskriminatorna*** ni ***arbitrarna***, te ih se mora moći ***osporiti*** i moraju biti podložna ***učinkovitim pravnim lijekovima***) te, podrobnije, moraju biti **dostupna** (tj. ***objavljena***) i dostatno **jasna** i **precizna** da bi bila "***predvidljiva***" u svojoj primjeni.[223]

Pozivanje na "poštivanje **biti**" prava i sloboda u pitanju mora se tumačiti kao **zabrana bilo kojeg zakonskog pravila koje bi tako duboko pogodilo neko pravo da bi ga time učinilo jalovim**. Primjerice, Sud Europske unije zauzeo je stav da:[224]

> Zakonodavstvo koje dopušta javnim vlastima da na općenitoj razini imaju pristup sadržaju elektroničkih komunikacija mora se smatrati da kompromitira bit temeljenog prava na poštivanje privatnog života, koje je zajamčeno člankom 7 Povelje…

Odstupanja država članica, naročito sukladno članku 23. GDPR-a – uključujući odstupanja od pravila o zaštiti podataka kako bi se zaštitila nacionalna sigurnost i obrana – ne smiju stoga nikada dovesti do takvih ničime zajamčenih i nikada prihvaćenih pretjeranih odstupanja od glavnih pravila.

Pobliže, bilo koja odstupanja sukladno članku 23., kao doista i bilo koja druga odstupanja od bilo kojih uobičajenih pravila u GDPR-u temeljem bilo kojih drugih posebnih klauzula, moraju udovoljavati testu "**nužna[e] i razmjerna[e] mjera[e] u demokratskom društvu**". To znači da bilo koje odstupanje od uobičajenih pravila ili ograničenja kod bilo kojeg neapsolutnog prava ispitanika, temeljem posebne klauzule, mora stvarno težiti zahtijevanom "***zakonitom cilju***"/"***važnom cilju od javnog interesa***", odgovarati na "***hitnu socijalnu potrebu***", te biti "***razumno razmjerno***" toj potrebi. Kod ocjenjivanja što je točno potrebno u tom smislu, državama se može odobriti određena "***razina diskrecije***"[225] – ali je ova razina ograničena zahtjevom da ta mjera (odstupanje ili ograničenje) mora biti nužna "***u demokratskom društvu***".

Općenito govoreći, ako postoji **jasna smjernica** o određenom pitanju – što je primjerice bio slučaj s Direktivom o zaštiti podataka iz 1995. g. putem Radne skupine iz članka 29 i ENZP-a, a sada se nudi sukladno GDPR-u od strane Europskog odbora za zaštitu podataka – (koji uključuje Europskog nadzornika, ENZP-a) – i/ili ako postoji **zamjetna usklađenost gledišta** o dotičnom pitanju između država članica (ili TZP-ova država članica), da će bilo koji otklon od takvih smjernica ili koncensus jedne države članice vjerojatno ukazati na to da mjere otklona (odstupanja ili ograničenja koja prelaze ono što se smatra potrebnim ili razmjernim u drugim državama članicama) nisu "nužne" ili "razmjerne" "u demokratskom društvu".

Međutim, kako je opisano pod sljedećim naslovom, ova pitanja ne mogu se riješiti pomoću "mehanizama suradnje i konzistentnosti" (opisano odvojeno, kasnije u tekstu).

PROBLEMI NASTALI POSEBNIM KLAUZULAMA

Obrazlagali smo do nekog stupnja detaljnosti o posebnim klauzulama jer one predstavljaju probleme za učinkovitu primjenu GDPR-a. Problemi se javljaju u dva oblika.

Prije svega, "fleksibilne" odredbe će po svojoj prirodi dovesti do **različitih (ili više ili manje detaljnih) pravila o identičnim pitanjima u različitim državama članicama**. Ovo ne predstavlja toliko problem u odnosu na obradu koja se odvija u cijelosti unutar jedne države članice, odnosno obradu koja se odnosi samo na ispitanike u toj državi članici. Međutim, kako je prethodno navedeno, u 21. stoljeću, sve više i više državnih

223 Vidjeti: Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights (Pravo Europske konvencije o ljudskim pravima), 2nd ed., 2009, Poglavlje 8, odlomak 3, *Ograničenja*. Za jednostavan pregled relevantnih zahtjeva koje propisuje EKLJP, vidjeti: Douwe Korff, The standard approach under articles 8 – 11 ECHR and article 2 ECHR (Standardan pristup prema člancima 8 – 11 EKLJP-a i članka 2 EKLJP-a) (nastavni materijal), dostupno na: https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8-11_ART2.pdf Vidjeti posebno tekst pod pitanjima 3 (Pravo) i 5 (Nužno i razmjerno) u tom materijalu.

224 *Maximillian Schrems v. Data Protection Commissioner*, presuda SEU-a u predmetu C-362/14, 6. prosinca 2015. g., odlomak 94.

225 Doktrina "razine diskrecije" ("*margin of appreciation*"), koja je snažno ugrađena u sudsku praksu Europskog suda za ljudska prava, manje je jasno iskazana pred Sudom Europske unije, koji se, ako ništa drugo, poziva na "diskreciju" ili "margin of discretion" dodijeljenu državama članicama u određenim pitanjima. Ali za potrebe ovog priručnika, može se smatrati da se doktrina ogleda u sudskoj praksi i sudova u Strasbourgu i u Luxembourgu, iako možda u donekle različitim stupnjevima i donekle ovisno o kontekstu. Vidjeti: Francisco Javier Mena Parras, From Strasbourg to Luxembourg? Transposing the margin of appreciation concept into EU law (Od Strasbourga do Luxembourga? Transponiranje koncepta "razine diskrecije" u EU pravo), Brussels, 2008, dostupno na: http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law__2015-7.pdf

aktivnosti ima međunarodne implikacije i uključuje prekogranične postupke obrade osobnih podataka, također i u javnom sektoru, a ne samo u odnosu na pitanja provedbe zakona ili ograničenja. Ovo je posebno slučaj unutar EU-a, jer su "četiri slobode", koje su temeljne za europski projekt: sloboda kretanja robe, usluga ljudi i kapitala.

Kada se roba ili usluge nude i kupuju preko granica, unutar EU-a, bez iznimke se prenose i osobni podaci koji slijede (i ključni su za) transakcije. Kada se ljudi kreću, to čine i njihovi podaci: njihovi podaci o porezu, socijalni i mirovinski doprinosi, njihovi medicinski podaci, podaci o bračnom statusu, rođenju, razvodu, smrti i evidencije o adresama stanovanja. Kad se vrše plaćanja (između pojedinaca ili između pojedinaca i pravnih osoba, ili između pojedinaca i državnih agencija/tijela, bilo da se radi o poreznim tijelima, tijelima koja vode evidencije o boravištu ili mirovinskim tijelima), to uključuje protok njihovih financijskih i drugih podataka. Ovo je *a fortiori* kada se obrada, ili dio obrade, odvijaju *online*, u internetskom okruženju.

Kada, u takvim okolnostima, postoje različita pravila u različitim državama članicama kojih se tiče obrada dotičnih podataka, ovo daje povoda potencijalnim (i potencijalno ozbiljnim pravnim pitanjima koja će se morati rješavati od slučaja do slučaja (što često neće biti jednostavno). Sljedeći primjeri mogu ilustrirati navedeno s referencom na neka specifična odstupanja i ograničenja koja se mogu uvesti temeljem prethodno spomenutih posebnih klauzula:

Primjeri:

- Ako jedna država članica nametne ograničenja na korištenje nacionalnog identifikacijskog broja, što nije propisano u drugoj državi članici, trebaju li se ta ograničenja i dalje primijeniti na primatelja u potonjoj državi članici (uključujući primatelja iz javnog sektora) ako se broj prenese tom primatelju?
- Ako jedna država članica nametne "daljnje uvjete" ili dodatna "ograničenja" obrade svih ili određenih vrsta osjetljivih podataka (npr. na korištenje biometrijskih ili genetskih podataka) koji nisu propisani u drugoj državi članici, jesu li ti uvjeti ili ograničenja i dalje primjenjivi na primatelja u potonjoj državi članici (uključujući primatelja iz javnog sektora) ako se podaci prenesu tom primatelju?
- Ako jedna država članica nametne dobnu granicu za privolu kod korištenja informacijskih usluga za djecu starosti, recimo, 14 godina, a druga država članica ostavi dobnu granicu na 16 godina, predloženu GDPR-om, može li pružatelj informacijskih usluga u prvospomenutoj državi članici pružati svoju uslugu djetetu starom 14 godina u potonjoj državi članici, na temelju privole 14-godišnjeg djeteta? Bi li pružatelj usluga trebao razlikovati na temelju IP-adrese djeteta (iako se to može lako "krivotvoriti" pomoću VPN-a, jer to čak mogu i 14-godišnjaci)?
- Ako jedna država članica traži pribavljanje prethodnog odobrenja od TZP-a za obradu u odnosu na socijalnu zaštitu i javno zdravlje, ali druga država članica to ne učini, može
- li javno tijelo u potonjoj državi članici obrađivati osobne podatke u odnosu na ispitanike u prvospomenutoj državi u takve svrhe, bez takvog prethodnog odobrenja – što bi se lako moglo dogoditi u odnosu na djecu migranata koji ostavljaju svoje supružnike i djecu u svojoj matičnoj državi dok za to vrijeme rade u drugoj državi članici, ali pri čemu se dječji doplatak npr. plaća supružnicima u matičnoj državi? (NB: u kontekstu pružanja takvog odobrenja, odgovarajući TZP će vjerojatno nametnuti ili zatražiti nametanje određenih zaštitnih mjera i ograničenja. Mora li i državna agencija u drugospomenutoj državi poštivati to isto? Bi li agencija uopće bila više svjesna takvih ograničenja?)

Gore navedena pitanja dodatno su otežana **zbog nepostojanja odredbe o "mjerodavnom pravu" u GDPR-u**, za razliku od odredbe sadržane u Direktivi o zaštiti podataka iz 1995. g. (čak iako ta odredba, iz članka 4, postavlja pitanja u odnosu na različite jezične prijevode i u pogledu učinkovitosti[226]Vjerojatno, takva je odredba izostavljena iz GDPR-a jer se pretpostavljalo da bi se odredba primijenila, s obzirom da se radi o uredbi, u cijelosti na usklađen način – ali, kako je prikazano prethodno u tekstu, u (mnogim) područjima obuhvaćenima "fleksibilnim" odredbama (kojima se trebaju baviti posebni zakoni na nacionalnoj razini) ovo očigledno neće biti slučaj.

Drugo pitanje odnosi se na **sukladnost sa zahtjevima vladavine prava** kako je izloženo ranije, pod prethodnim podnaslovom. Pitanja će se vjerojatno javiti o tome zadovoljavaju li određeni zakoni u određenim državama članicama, koji ograničavaju određena prava ili olabavljuju različita pravila, taj test, tj. jesu li dostatno dostupni, precizni i predvidljivi u svojoj primjeni, potrebni ili razmjerni odnosnom (legitimnom/važnom) cilju.

Ta pitanja često se ne mogu riješiti, čak ni podvesti, pod "mehanizmima suradnje i konzistentnosti" o kojima se govori kasnije u tekstu, jer ti su mehanizmi ograničeni na suradnju vezano za mjere poduzete ili predložene za poduzimanje od strane tijela za zaštitu podataka: ne mogu se koristiti za ispravljanje manjkavosti u zakonima država članica. Ovo može stvoriti ozbiljne probleme, posebno u odnosu na prijenose osobnih podataka od jedne državne agencije u jednoj državi članici na drugu državnu agenciju u drugoj državi članici, ako ova potonja navede da će podaci biti obrađeni prema zakonima koji navodno ne zadovoljavaju zahtjeve vladavine prava. Ipak, iskustvo u drugim područjima (kao što su pravila za pravosuđe i unutarnje poslove, nisu raspravljeni u prvom izdanju ovog priručnika) pokazuje da se, kada je to potrebno, može pokrenuti akcija za rješavanje takvih pitanja, posebno na osnovi prijedloga Komisije ili EOZP-a.

IMPLIKACIJE ZA SZP-OVE

Treba biti jasno iz gore navedenoga da bi SZP-ovi trebali biti svjesni, i **proučiti, ne samo pravila iz GDPR-a, već također i bilo koja relevantna nacionalna pravila koja se grade na posebnim klauzulama iz GDPR-a** – a u nekoj mjeri i doista relevantne zakone i pravila u drugim državama članicama i u trećim zemljama, ako njihova organizacija otkriva osobne podatke takvim drugim državama.

Ovo se može u nekoliko oblika. U nekim slučajevima, države članice mogu jednostavno zadržati pravila koja su postojala prije nego li je GDPR stupio na snagu, uključujući posebna odstupanja (derogacije) za zaštitu važnih javnih interesa, ili radi olakšavanja istraživanja – premda **ova pravila ne moraju uvijek nužno udovoljavati zahtjevima vladavine prava relevantnih posebnih klauzula niti biti "prikladna" ili "odgovarajuća" u smislu GDPR-a** (kako je prethodno objašnjeno u tekstu). U drugim slučajevima, njihova država članica je moguće usvojila posebne zakone ili zakonita pravila da bi "dalje regulirala" pitanja koja su prepuštena državama članicama prema GDPR-u, ili da bi pojasnila koje su opcije korištene itd. U nekim drugim pak slučajevima, država članica možda još uopće nije razjasnila nacionalnu primjenu određenih posebnih klauzula.

SZP-ovi mogu naravno sami ispraviti bilo koje manjkavosti ili pitanja u tom smislu. Međutim, unutar vlastite mreže SZP-ova, i u njihovih interakcija sa svojim nacionalnim tijelima za zaštitu podataka,[227] oni mogu **upozoriti za takva pitanja i potaknuti prikladnu akciju**. Oni također trebaju – ponovo, po mogućnosti, zajedno sa svojim drugim SZP-ovima koji rade u sličnim organizacijama – **alarmirati više strukture u svojim vlastitim organizacijama** (u javnom sektoru, primjerice, relevantnog(e) ministra(ministre)) na takve primijećene manjkavosti. U takvim situacijama, SZP-ovi moraju razviti strateški učinkovite pristupe.

226 Vidi Douwe Korff, *The question of "applicable law"*, u: Compliance Guide 3 – Interim report, Privacy Laws & Bussines, studeni 1999.
227 Usp. **francuski** SZP "Extranet" koji može biti koristan u takvim kontekstima. Vidjeti bilješku (fusnotu) 97, prethodno u tekstu.

2.3. OPĆI PREGLED GDPR-A

U nastavku slijedi opći pregled GDPR-a, nižu se poglavlja jedno za drugim, odjeljak po odjeljak, odnosno članak po članak.

* Nadamo se da će se za budućnost, prošireno drugo izdanje ovog priručnika, izraditi kratki članak po članak o svim odredbama o GDPR-u, koji će se usredotočiti na konkretnu, praktičnu primjenu relevantnih odredbi. U međuvremenu, organizacijama osoba s invaliditetom se savjetuje da prouče jedan od glavnih akademskih komentara koji se objavljuje na nekoliko jezika, kao i, naravno, službene smjernice koje izdaju nacionalna tijela za zaštitu prava, EOZP i nacionalni i europski sudovi.

2018 OPĆA UREDBA O ZAŠTITI PODATAKA:

POGLAVLJE I:

Opće odredbe (članci 1. – 4.)

- Predmet i ciljevi Uredbe;
- Materijalno područje primjene;
- Teritorijalno područje primjene;
- Definicije.

POGLAVLJE II:

Načela (članci 5. - 11.):

- Načela koja se odnose na obradu osobnih podataka;
- Zakonitost obrade [pravne osnove];
- Uvjeti privole;
- Uvjeti koji se primjenjuju na djetetov pristanak u vezi s uslugama informacijskog društva;
- Obrada posebnih kategorija osobnih podataka [osjetljivi podaci];
- Obrada osobnih podataka koji se odnose na kaznene osude i kažnjiva djela;
- Obrada koja ne zahtijeva identifikaciju.

POGLAVLJE III:

Prava ispitanika

Odjeljak 1 (članak 12.)

Transparentnost i modaliteti:

- transparentne informacije, komunikacije i modaliteti za ostvarivanje prava ispitanika.

Odjeljak 2 (članci 13. – 15.):

Informacije i pristup osobnim podacima:

- Informacije koje treba dostaviti ako se osobni podaci prikupljaju od ispitanika;
- Informacije koje treba pružiti ako osobni podaci nisu dobiveni od ispitanika;
- Pravo ispitanika na pristup.

Odjeljak 3 (članci 16. – 20.):

Ispravak i brisanje:

- Pravo na ispravak;
- Pravo na brisanje ("pravo na zaborav");
- Pravo na ograničenje obrade [];
- Obveza izvješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade;
- Pravo na prenosivost podataka.

Odjeljak 4 (članci 21. – 22.)

Pravo na prigovor i automatizirano pojedinačno donošenje odluka

- Pravo na prigovor;
- Automatizirano individualno donošenje odluka, uključujući profiliranje.

Odjeljak 5 (članak 23.)

Ograničenja

POGLAVLJE IV:

Voditelj obrade i izvršitelj obrade

Odjeljak 1 (članci 24. – 31.)

Opće obveze:

- Obveze voditelja obrade;
- Tehnička i integrirana zaštita podataka;
- Zajednički voditelji obrade;
- Predstavnici voditelja obrade ili izvršitelja obrade koji nemaju poslovni nastan u Uniji;
- Izvršitelj obrade;
- Obrada pod vodstvom voditelja obrade ili izvršitelja obrade;
- Evidencija aktivnosti obrade;
- Suradnja s nadzornim tijelom.

Odjeljak 2 (članci 32. – 34.)

Sigurnost osobnih podataka:

- Sigurnost obrade;
- Izvješćivanje nadzornog tijela o povredi osobnih podataka;
- Obavješćivanje ispitanika o povredi osobnih podataka.

Odjeljak 3 (članci 35. – 36.)

Procjena učinka na zaštitu podataka i prethodno savjetovanje:

- Procjena učinka na zaštitu podataka;
- Prethodno savjetovanje.

Odjeljak 4 (članci 37. – 39.)

Službenik za zaštitu podataka:

- Imenovanje službenika za zaštitu podataka;
- Radno mjesto službenika za zaštitu podataka;
- -Zadaće službenika za zaštitu podataka.

Odjeljak 5 (članci 40. – 43.)

Kodeksi ponašanja i certificiranje:

- Kodeksi ponašanja;
- Praćenje odobrenih kodeksa ponašanja;
- Certificiranje;
- Certifikacijska tijela.

POGLAVLJE V (članci 44. – 50.):

Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama:

- Opća načela prijenosa;
- Prijenosi na temelju odluke o primjerenosti;
- Prijenosi koji podliježu odgovarajućim zaštitnim mjerama;
- Obvezujuća korporativna pravila;
- Prijenos ili otkrivanje podataka koji nisu dopušteni u pravu Unije;
- Odstupanja za posebne situacije;
- Međunarodna suradnja s ciljem zaštite osobnih podataka.

POGLAVLJE VI:

Neovisna nadzorna tijela

Odjeljak 1 (članci 51. – 54.):

Neovisni status:

- Nadzorno tijelo;
- Neovisnost;
- Opći uvjeti za članove nadzornog tijela;
- Pravila za osnivanje nadzornog tijela.

Odjeljak 2 (članci 55. – 59.)

Nadležnost, zadaće i ovlasti:

- Nadležnost;
- Nadležnost vodećeg nadzornog tijela;
- Zadaće;
- Ovlasti;
- Izvješća o aktivnostima.

POGLAVLJE VII:
Suradnja i konzistentnost

Odjeljak 1 (članci 60. – 62.):
Suradnja:

- Suradnja vodećeg nadzornog tijela i drugih predmetnih nadzornih tijela;
- Uzajamna pomoć;
- Zajedničke operacije nadzornih tijela.

Odjeljak 2 (članci 63. – 67.)
Konzistentnost:

- Mehanizam konzistentnosti;
- Mišljenje Odbora;
- Rješavanje sporova pri Odboru;
- Hitni postupak;
- Razmjena informacija.

Odjeljak 3 (članci 68. – 76.)
Europski odbor za zaštitu podataka:

- Europski odbor za zaštitu podataka;
- Neovisnost;
- Zadaće Odbora;
- Izvješća;
- Postupak;
- Predsjednik;
- Zadaće predsjednika;
- Tajništvo;
- Povjerljivost.

POGLAVLJE VIII (članci 77. – 84.):
Pravna sredstva, odgovornost i sankcije:

- Pravo na pritužbu nadzornom tijelu;
- Pravo na učinkoviti pravni lijek protiv nadzornog tijela;
- Pravo na učinkoviti pravni lijek protiv voditelja obrade ili izvršitelja obrade;
- Zastupanje ispitanika;
- Suspenzija postupka;
- Pravo na naknadu štete i odgovornost;
- Opći uvjeti za izricanje upravnih novčanih kazni;
- Sankcije.

POGLAVLJE IX (članci 85. – 91.):

Odredbe u vezi s posebnim situacijama obrade:

- Obrada i sloboda izražavanja i informiranja;
- Obrada i javni pristup službenim dokumentima;
- Obrada nacionalnog identifikacijskog broja;
- Obrada u kontekstu zaposlenja;
- Zaštitne mjere i odstupanja vezano za obradu u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe;
- Obveze tajnosti;
- Postojeća pravila o zaštiti podataka crkava i vjerskih udruženja.

POGLAVLJE X (članci 92. – 93.):

Delegirani akti i provedbeni akti:

- Izvršavanje delegiranja ovlasti;
- Postupak odbora.

POGLAVLJE XI (članci 94. – 99.):

Završne odredbe:

- Stavljanje izvan snage Direktive 95/46/EZ;
- Odnos s Direktivom 2002/58/EZ;
- Odnos s prethodno sklopljenim sporazumima;
- Izvješća Komisije;
- Preispitivanje drugih akata Unije o zaštiti podataka;
- Stupanje na snagu i primjena.

2 .4 NAČELO POUZDANOSTI [ODGOVORNOSTI][228]

2.4.1 Nova obveza dokazivanja sukladnosti s Uredbom

Premda se može činiti da nije ništa novo, ovo je zapravo jedna od glavnih značajki nove EU Opće uredbe o zaštiti podataka (GDPR) – moguće čak i *doista* glavna značajka – to što stavlja veliki naglasak na činjenicu da:

> **Voditelj obrade odgovoran je za *usklađenost s* [načelima koja se odnose na obradu osobnih podataka] […] te je mora biti u mogućnosti *dokazati* ('pouzdanost' ['odgovornost'])** (čl. 5(2)).

Kako navodi talijansko tijelo za zaštitu podataka, *Garante del Privacy*: [229]

> Učiniti pravnu osobu *odgovornom* znači zadati [u zadatak] radnje i odluke tom tijelu **i očekivati da tijelo odgovara za te radnje i odluke.** Stoga, odgovornost je **stanje u kojem je nametnuta odgovornost** za radnje i odluke koje su tijelu dodijeljene.

Novost koncepta ne leži u odgovornosti tijela nadležnog za obradu odgovarati za usklađenost – to je naravno već također bio slučaj prema Direktivi o zaštiti podataka iz 1995. g. (premda ta direktiva ne koristi termin "pouzdanost" / ["odgovornost"]). Naime, novost je naglasak na tome da se traži od voditelja obrade (a u nekim slučajevima od izvršitelja obrade) da "**dokaže**" ovu usklađenost: Uredba koristi ovaj izraz čak 33 puta.

Ovo se razlikuje od Direktive iz 1995. g. koja nigdje izrijekom ne traži od "nadzornika" [pandan voditelju obrade iz GDPR-a] ili "obrađivača" [pandan izvršitelju obrade iz GDPR-a] da dokažu usklađenost s bilo čime. Podrobnije, različite sheme "obavješćivanja" ili "registracije" utemeljene na Direktivi barem u nekim državama nisu mnogo učinile za dokazivanje takve usklađenosti,[230] dok su u drugima bile uspješne utoliko što su bile vrlo detaljne i prikazane na takav način da potaknu voditelje obrade prema ispunjavanju svih zakonskih zahtjeva za bilo koji novi postupak obrade, pri čemu je nadležno tijelo za zaštitu podataka (TZP) upozoravalo voditelja obrade i predlagalo modifikacije ili davalo savjete kada je to nužno ili potrebno. U kontekstu brzo širećih i evoluirajućih praksi obrade podataka, i u državama (kao što su države članice EU-a) gdje je već postojalo neko zamjetno znanje i iskustvo s primjenom načela i pravila o zaštiti podataka, također u kontekstu promocije "društvene odgovornosti" organizacija, opravdan je bio novi pristup koji naglašava primarnu odgovornost i odgovornost onih koji obrađuju osobne podatke (bilo u svojstvu "voditelja obrade" ili "izvršitelja"). To je objašnjenje što zapravo predstavljaju načelo pouzdanosti [odgovornosti] i dužnost dokazivanja.

Kako se obrazlaže pod točkom 2.3, dalje u tekstu, Uredba traži imenovanje Službenika za zaštitu podataka (SZP-a) za sve voditelje obrade podataka iz javnog sektora i za mnoge iz privatnog sektora, kao glavno institucionalno sredstvo da bi se načelo pouzdanosti [odgovornosti] primijenilo u praksi.

Kao što prethodno citirana odredba o načelu pouzdanosti [odgovornosti] iz čl. 5(2), jasno izražava, obveza dokazivanja usklađenosti prvenstveno se primjenjuje na sva temeljna načela koja su u temelju Uredbe, a navedena su u čl. 5(1), konkretno zakonitost, poštenost i transparentnost; uska i izričita specifikacija svrhe i ograničavanje svrhe; smanjenje količine podataka (uključujući primjerenost, relevantnost i nužnost podataka); točnost (uključujući ažurnost); ograničenje (zadržavanja) pohrane; cjelovitost, povjerljivost i sigurnost. Naravno,

228 Ovaj odlomak oslanja se rad, a dijelom ga i ponavlja, odnosno sumira, autora Douwe Korff, The Practical Implications of the new EU General Data Protection Regulation for EU- and non-EU Companies (Praktične implikacije nove EU Opće uredbe o zaštiti podataka za društva iz EU i izvan EU-a), kolovoz 2016., rad prezentiran na CMS Cameron McKenna LLP, London, u veljači 2017. g., dostupno na: http://ssrn.com/abstract=3165515

229 Luigi Carrozzi, prezentacija za prvi edukacijski sastanak "T4DATA", lipanj 2018. g., slajd na temu "*Asset inventory and the Accountability Principle*" (izvorni naglasci).

230 Vidi GDPR, Uvodna izjava 89.

to vrijedi i za (ako ništa drugo, onda *a fortiori*) na posebno strogu primjenu tih načela kod obrade koja uključuje posebne kategorije podataka (tzv. osjetljivi podaci – čl. 9) ili na drugi način predstavlja visok rizik za prava i slobode fizičkih osoba (i koji stoga zahtijevaju posebnu procjenu učinka na zaštitu podataka – čl. 35).

Izvan ovoga, Uredba izrijekom ili implicitno nameće obvezu dokazivanja sukladnosti u mnogo više specifičnih konteksta, uključujuću i one u odnosu na:

- Pribavljanje privole ispitanika (kada je potrebna) (vidjeti čl. 7(1));
- Odbijanje zahtjeva ispitanika za pristup ili ispravak podataka (vidjeti čl. 11(2) i 12(5));
- Neusklađenost s ispitanikovim prigovorima na obradu podataka (vidjeti čl. 21(1));
- Da izvršitelji i njihovi podizvođači (pod-izvršitelji) "u dovoljnoj mjeri jamče" svoju stručnost i poduzimanje "odgovarajućih tehničkih i organizacijskih mjera" da se osigura sigurnost obrade podataka (vidi čl. 28 i 32);
- Pružanje "odgovarajuće[ih] zaštitne[ih] mjere[a]" za prijenose osobnih podataka u treće zemlje bez primjerene zaštite podataka (čl. 46);
- itd.

Usko povezana s ovom obvezom dokazivanja sukladnosti su nove opće i posebne obveze koje GDPR nameće u smislu:

- **izrade evidencije operacija obrade osobnih podataka**;
- provođenja **općeg pregleda tih aktivnosti**;
- **procjene rizika** za prava i slobode pojedinaca koje predstavljaju te operacije;
- provođenja dubinskih **procjena učinka na zaštitu podataka** u odnosu na operacije za koje se procjenjuju da bi mogle rezultirati **"visokim rizikom";**
- korištenja **tehničke i integrirane zaštite podataka** u odnosu na sve operacije obrade osobnih podataka;
- zahtjeva **obavješćivanja o kršenju podataka**.

Razmotrit ćemo sve njih, a posebno uloge SZP-a u odnosu na njih, u pojedinostima u trećem dijelu. Stoga ovdje mogu biti dovoljne kratke napomene i upućivanja na taj dio.

Stoga, kao prvo, Uredba nameće ključni **opći zahtjev da se vodi detaljna evidencija svih operacija obrade osobnih podataka voditelja obrade**, navodeći specifične pojedinosti svake pojedine operacije (čl. 30); te bi **se evidencije trebale voditi u registru postupaka obrade osobnih podataka** i moraju pokazati da i kako se poštuju gore navedene opće obveze i sve specifičnije (usp. uvodnu izjavu 82). Vidi raspravu o zadatku 1 u trećem dijelu ovog priručnika.

Drugo, Uredba zahtijeva od voditelja, uz pomoć svojih SZP-ova, da **preispitaju svoje poslovanje** i prema potrebi ih usklade s Uredbom, te da zabilježe pregled i sve korektivne mjere poduzete u gore navedenom registru. Vidi raspravu o zadatku 2 u trećem dijelu ovog priručnika.

Treće, Uredba nameće opću obvezu voditeljima da "uzmu u obzir" **rizike** koje predstavlja predloženi postupak obrade voditelja, zajedno s obvezom provođenja "*odgovarajućih tehničkih i organizacijskih mjera*" kako bi se suprotstavili tim rizicima i obvezu "*pokazati da se obrada provodi u skladu s ovom Uredbom*" - tj. Uredba zahtijeva da su ti rizici doista ocijenjeni i da su mjere poduzete u svjetlu te procjene bile prikladne za te rizike (članak 24, stavak 1; usporedi i čl. 24) 32) te ove stvari treba uredno zabilježiti. Vidi raspravu o zadatku 3 u trećem dijelu ovog priručnika.

Četvrto, ako opća procjena rizika (navedeno gore) pokaže da postoji vjerojatnost **visokog rizik**a za prava i slobode fizičkih osoba, voditelj mora prije obrade provesti **procjenu učinka zaštite podataka (PUZP)** predviđene obrade o zaštiti osobnih podataka i dokumentirati tu procjenu. Dokument PUZP-a mora sadržavati:

sustavni opis predviđenih postupaka obrade i svrhe obrade; procjenu nužnosti i razmjernosti postupaka obrade i podataka u odnosu na te svrhe; procjenu rizika za prava i slobode subjekata podataka koje predstavlja obrada; i opis mjera predviđenih za rješavanje tih rizika, uključujući *"mjere zaštite, sigurnosne mjere i mehanizme kojima se osigurava zaštita osobnih podataka i dokazivanje sukladnosti s ovom Uredbom uzimajući u obzir prava i legitimne interese ispitanika i drugih zainteresiranih osoba*" (čl. 35). Vidi raspravu o zadatku 4 u trećem dijelu ovog priručnika.

Peto, Uredba nameće opću obvezu voditeljima da koriste **"tehničku i integriranu zaštitu",** kako u postavljanju tako i u obavljanju svih operacija obrade voditelja (čl. 25) - i voditelj mora moći dokazati da je to učinjeno. U tom smislu, u Uredbi se navodi da se certifikati (pečati za zaštitu podataka) mogu koristiti kao "element" za dokazivanje sukladnosti (članak 25, stavak 3, koji se dalje razmatra u nastavku). Vidi raspravu o zadatku 9 u trećem dijelu ovog priručnika.

I šesto, voditelji moraju **zabilježiti/dokumentirati sve pojedinosti o svim povredama osobnih podataka** (povrede sigurnosti osobnih podataka) i poduzete korektivne mjere te **obavijestiti** nadležna (nadležna) nadzorna tijela o tim pojedinostima u roku od 72 sata (čl. 33). Ispitanici na koje se odnosi kršenje također moraju biti obaviješteni, ali samo ako je "povreda osobnih podataka vjerojatno rezultirala visokim rizikom za [njihova] prava i slobode", te u manje specifičnim detaljima (čl. 34). Vidi raspravu o zadatku 6 u trećem dijelu ovog priručnika.

Uredba također sadrži neke specifičnije obveze evidentiranja, uključujući i odredbu da ako dva ili više voditelja zajednički odrede svrhu i sredstva obrade, oni su zajednički voditelji. Kao takve, one moraju "na transparentan način odrediti svoje odgovornosti za ispunjavanje obveza iz ove Uredbe" u obliku **"dogovora između njih**"; i ovaj "dogovor" "propisno odražava odgovarajuće uloge i odnose zajedničkih voditelja u odnosu na ispitanika". U praksi, budući da nadzorna tijela mogu zatražiti od voditelja da dokaže usklađenost s tim obvezama, sporazum mora biti u **pisanom obliku ili u usporedivo pouzdanom elektroničkom obliku** (čl. 26).

I naravno, različite odredbe u Uredbi koje zahtijevaju od voditelja obrade, zajedničkih voditelja obrade, izvršitelja obrade i podizvršitelja da odrede dogovore između njih i/ili u vezi s prijenosom podataka u **ugovorima ili sličnim pravno obvezujućim instrumentima** također zahtijevaju dokumentaciju.

2.4.2 Načini dokazivanja sukladnosti

Opća obveza vođenja detaljnih **evidencija**, a posebice obveza evidencije za zajedničke voditelje obrade, povrede podataka i PUZP-ovi, spomenuti prethodno u tekstu, predstavljaju glavne, općenite načine dokazivanja sukladnosti, predviđene u Uredbi.

Te evidencije bi trebale odražavati opću kulturu i pristup promicanja zaštite podataka, koji se odražava na takve **prakse** kao što su:

- osmišljavanje i formalno usvajanje internih politika zaštite podataka (i poduzimanje povezanih akcija, kao što su edukacije);
- usvajanje načela tehničke i integrirane zaštite podataka u svim aktivnostima obrade podataka voditelja obrade, u svim njegovim proizvodima i uslugama, na svakom koraku, od njihovog koncipiranja sve do njihovog ostvarenja;
- minimiziranje korištenja i zadržavanja osobnih podataka, a podrobnije rečeno – korištenje i dalje prepoznatljivih podataka (koristeći pseudonimizaciju ili anonimizaciju prethodno prepoznatljivih podataka kad god je to moguće);
- osiguravanje najveće moguće transparentnosti o aktivnostima obrade voditelja obrade u odnosu na ispitanike i opću javnost, u papirnim obrascima, elektroničkim obrascima, te izloženo na jasan način i u podrobnijim izjavama o privatnosti i zaštiti podataka na mrežnim stranicama (npr. jasno razlikujući,

izravno na stranici s koje se prikupljaju osobni podaci, između toga što su obvezna i izborna polja/svrhe i podaci, te omogućujući mnogo veću mogućnost legitimnog izbora za korisnike mrežnih stranica, označavanjem (klikom) na određenu kućicu) te ustanovljavanja djelotvornih i učinkovitih sredstava za rješavanje zahtjeva ispitanika za dobivanje općih ili specifičnih informacija; i

- osiguravanje da voditelj obrade sam može nastaviti učinkovito nadzirati aktivnosti, posebice što se tiče sigurnosti (pomoću zapisa o pristupu i promjenama itd.; te da je u mogućnosti pojačati sigurnosti kad god je to potrebno (npr., izdavanjem "zakrpa" ("*patches*").

(Usp. Uvodna izjava 78)

U trećem dijelu, dodatno ćemo, i mnogo detaljnije, razmotriti sva ova pitanja, s konkretnim primjerima i praktičnim smjernicama o tome kako izvršavati gornje zadaće.

Ali, osim toga, prethodna uvodna izjava (77) navodi različite **posebne načine** za dokazivanje poštivanje odredaba, tj.:

- postupanje sukladno odobrenim kodeksima ponašanja;
- postupanje sukladno odobrenim certifikatima;
- postupanje sukladno smjernicama koje pruža Europski odbor za zaštitu podataka; i naravno:
- postupanje sukladno naznakama koje pruža službenik za zaštitu podataka.

Ovome se može dodati, posebno u odnosu na prekogranične prijenose i dijeljenje osobnih podataka:

- obvezujuća korporativna pravila (OKP-ovi);
- administrativni dogovori ("aranžmani") između tijela javne vlasti ili javnih tijela; i
- standardni ili individualno odobreni ugovori o prijenosu podataka.

U odnosu na povrede podataka, obavještavanje (i pojedinosti sadržane u obavijesti) mogu se također smatrati posebnim načinima za dokazivanje sukladnosti s traženim uvjetima.

Međutim, treba naglasiti da u odnosu na sve navedeno, iako mogu sačinjavati "elemente" u sveukupnom nastojanju da se iskaže usklađenost i "posebnim sredstvima" za to, oni ne predstavljaju nužni pravni dokaz usklađenosti.

2.4.3 Dokazna vrijednost različitih načina dokazivanja sukladnosti

U većini aspekata, poštivanje bilo kojeg od gore navedenih načina predstavlja "element za dokazivanje sukladnosti", tj. stvara presumpciju sukladnosti, ali ta je presumpcija oboriva. Ako tijelo za zaštitu podataka krene dalje istraživati neko pitanje, moglo bi utvrditi da, neovisno o formalnom poštivanju takvih smjernica, kodeksa, certifikacija, aranžmana, ugovora ili pravila, u specifičnom slučaju Uredba ipak nije bila poštivana (iako bi bilo koji dobronamjerni napor dokazivanja sukladnosti imao značajan učinak na mjeru bilo koje kazne, ako bi ista bila nametnuta – usp. čl. 83).[231]

231 Za detalje, vidjeti prvu stranicu Tablice u radu spomenutom u bilješci (fusnoti) 3, prethodno u tekstu (na str. 11).

2.5 SLUŽBENIK ZA ZAŠTITU PODATAKA (SZP)

2.5.1 Pozadina

Koncept o službenicima za zaštitu podataka koje je imenovao voditelj obrade iz javnog i privatnog sektora, dolazi iz njemačkog prava o zaštiti podataka, koje u propisima predviđa takve službenike već dugo vremena.[232] Čak i u državama koje nisu dužne prema Direktivi o zaštiti podataka iz 1995. g. imenovati SZP-ove sukladno zakonu (kao što je Austrija, koja u drugim aspektima često slijedi njemački primjer), ili su uključeni samo kao opcija (kao u Francuskoj) institucija SZP-a je postala široko prihvaćena. U nekoliko zemalja, postoje nacionalna udruženja SZP-ova, a postoji i Udruženje europskih organizacija za zaštitu podataka (*Confederation of European Data Protection Organisations, CESZP*), koja je izdala

"praktične smjernice za organizacije" o "odabiru najboljeg kandidata" za radno mjesto

SZP-a.[233] Na globalnoj razini, postoji Međunarodno udruženje profesionalaca u pitanjima privatnosti (*the International Association of Privacy Professionals, IAPP*) sa sjedištem u SAD-u, koje *inter alia* nudi certifikacije za zaštitu podataka "profesionalcima za pitanja privatnosti

informacija". Iako, kao i drugi programi certificiranja SZP-ova, oni ne predstavljaju certifikate usklađenja s GDPR-om: vidi odlomak 2.5.3, niže, pod naslovom "Formalno osposobljavanje i certificiranje [SZP-a]". *(Vidjeti popis udruženja SZP-a na kraju ovog pododlomka, s poveznicama na njihove mrežne stranice.)*

Direktiva o zaštiti podataka iz 1995. g. nije još tražila nadzornike [voditelje obrade] da imenuju SZP-ove. Umjesto toga, priznala je postojanje SZP-ova u pravu i praksi država članica, dopuštajući državama članicama da izuzmu voditelje obrade od obveze obavještavanja nadležnog tijela za zaštitu podataka (TZP) o postupcima obrade, ako pravo države članice zahtijeva od dotičnog voditelja obrad da imenuje SZP koji je "*posebno nadležan [ ] osigurati na neovisan način unutarnju primjenu nacionalnih odredbi donesenih u skladu s ovom Direktivom [i] voditi [a] evidenciju operacija obrade koje izvršava voditelj obrade, a sadrži [iste podatke o kojima bi inače bilo obaviješteno TZP]*" (čl. 18(2)).

Međutim, EU regulativa iz 2001. g. koja određuje pravila o zaštiti podataka za same EU institucije (Uredba (EZ) 45/2001)[234] zahtijeva od svake EU institucije ili tijela da imenuju barem jednog SZP-a (čl. 24). Pravila o SZP-ovima u EU institucijama, utjelovljena u ovoj uredbi, vrlo su slična onima iz GDPR-a.

Tzv. Direktiva o zaštiti podataka u provedbi zakona (*the Law Enforcement Data Protection Directive*) (Direktiva 2016/680),[235] usvojena u isto doba kao i GDPR, traži da "nadležna tijela" na koje se primjenjuje ta direktiva također imenuju SZP; a Smjernice RS29 o SZP-ovima (koje sadrže, kako je navedeno dalje u tekstu, glavne smjernice za SZP-ove koji su imenovani prema GDPR-u) naglašava da "[d]ok se ove smjernice fokusiraju na SZP-ove prema GDPR-u, smjernice su također relevantne u pogledu SZP-ova imenovanih sukladno Direktivi 2016/680, u odnosu na njihove slične odredbe".[236]

232 Njemački izrazi su: *behördliche-*, odnosno *betriebliche Datenschutzbeauftragter*. Za kratak sažetak njihove uloge i funkcija prema njemačkom pravu, vidjeti npr.: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
Za detaljnije izlaganje na njemačkom jeziku, vidjeti npr., Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG (Kratak komentar njemačkog saveznog prava o zaštiti podataka), 3. izdanje (2010), komentari na čl. 4f BDSG, ukupno 85 bilježaka, str. 187-213.

233 CEDPO, Choosing the best candidate as your Data Protection Officer (SZP) – Practical guidelines for organisations (Odabir najboljeg kandidata za Službenika za zaštitu podataka (SZP) – Praktične smjernice za organizacije, 30. svibnja 2016. g., dostupno na: http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-dataprotection-officer-dpo-practical-guidelines-for-organisations.html

234 Puni naziv: UREDBA (EZ) br. 45/2001 EUROPSKOG PARLAMENTA I VIJEĆA od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL L 8 of 12.1.2001, str. 1ff., dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32001R0045&from=HR

235 Puni naziv: Direktiva (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL L 119, 4.5.2016, str. 89ff., dostupno na: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

236 Radna skupina iz Članka 29, Guidelines on Data Protection Officers ('DPOs') Smjernice o službenicima za zaštitu podataka (SZP-ovima), izvorno usvojena 13. prosinca 2016. g., s posljednjim izmjenama i usvojena 5. travnja 2017. (WP243 RS243 rev.01), str. 4, bilješka (fusnota) 2., dostupno na: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Interni SZP-ovi u EU blisko surađuju s Europskim nadzornikom za zaštitu podataka (ENZP) i stvorili su Mrežu službenika za zaštitu podataka EU institucija i tijela (*the Network of Data Protection Officers of the EU Institutions and Bodies*). ENZP je oformio mrežnu stranicu, "DPO Corner" ("SZP kutak") da bi ih podržao. Nakon rada iz 2005. g. kojeg je sastavio ENZP,[237] Mreža je 2010. g. izdala zbirku naziva Profesionalni standardi za službenike za zaštitu podataka u EU institucijama i tijelima koji djeluju sukladno Uredbi (EZ) 45/2001.[238] ENZP je 2012. g. izdao izvješće o statusu SZP-ova, kao dio svog nadzora usklađenosti institucija s pravilima Uredbe (EZ) 45/2001.[239] Ovo izvješće "potvrđuje da je funkcija SZP-a sada dobro postavljena unutar EU institucija i tijela, te da su oni općenito sukladni s člankom 24. Uredbe", ali je također zamijetio postojanje "nekih zabrinjavajućih područja" koja podliježu daljnjem nadzoru ENZP-a.[240] Ovi dokumenti sadrže prilično opsežne smjernice o pitanjima relevantnima za imenovanje, položaj i zadaće SZP-ova.

U novije doba, i više izravno relevantno za ovaj Priručnik, Radna skupina članka 29. izradila je smjernice o SZP-ovima, kao dio pripreme za GDPR koji je uskoro stupao u primjenu.[242] Europski odbor za zaštitu podataka, koji je nastavio na radu RS29-a nakon stupanja GDPR-a u primjenu, formalno je podržao ove smjernice (kao i druge dokumente o pitanjima koja se javljaju vezano za GDPR, a koje je RS29 bio usvojio prije tog datuma).[241]

Kao posljedica toga, nekoliko nacionalnih TZP-ova je također izdalo smjernice o SZP-ovima, neki čak i prije GDPR-a, i time promovirali specifične usluge za njih.[242]

Trenutni odlomak Priručnika posebice se temelji na smjernicama RS29, ali također se poziva na druge smjernice prethodno navedene u tekstu, kada je to prikladno za obogaćivanje razumijevanja čitatelja.

Glavni naglasak u ovom uvodu vezan za funkciju SZP-a je da je to, u smislu GDPR-a, ključna nova institucija koja bi se trebala smatrati presudnim sredstvom za davanje praktičnog učinka načelu "pouzdanosti"/ ["odgovornosti"] (obveza dokazivanja sukladnosti), o kojem smo prethodno govorili: u slučajevima kada je SZP imenovan i savjesno obavlja svoje zadaće (kao što se govori u 3. dijelu ovog priručnika), to bi trebalo dovesti do bolje, opsežnije i ozbiljnije sukladnosti s GDPR-om negoli se postiglo putem vanjskog nadzora od strane tijela za zaštitu podataka u odnosu na Direktivu o zaštiti podataka iz 1995. g. Sada, prema GDPR-u, TZP-ovi imaju i izravnu kontakt osobu koja ima znanje o relevantnim pitanjima, i to unutar organizacije svih relevantnih voditelja obrade, a ujedno im je i saveznik unutar organizacije voditelja obrade. Nimalo iznenađujuće, sada kada je GDPR stupio u primjenu, nekoliko TZP-ova je kao svoj prioritet odlučilo provjeriti jesu li organizacije koje moraju imenovati SZP-ove (kako se dalje u tekstu objašnjava, pod točkom 2.3.2) doista to i učinile.[243]

Nadalje se ove Smjernice nazivaju: "**WP29 Guidelines on DPOs" ("Smjernice RS29 o SZOP-ovima")**

237 EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, dostupno na: https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf

238 https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf

239 EDPS, Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers (Praćenje sukladnosti EU institucija i tijela s Čl. 24 Uredbe (EZ) 45/2001 – Izvještaj o pravnom položaju DPO-ova), 17. prosinca 2012.g., dostupno na: https://edps.europa.eu/sites/edp/files/publication/2012-12-17_dpo_status_web_en.pdf

240 Idem, str. 3.

241 EDPB, Endorsement 1/2018, podupirući inter alia i Smjernice WP29 o DPO-ovima (WP29 Guidelines on DPOs) (navedeno kao 7. podržani dokument), usvojen 25.svibnja 2018.g., dostupno na: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

242 Pogledati, npr.: Guide de Correspondant Informatique et Libertés (CIL) (Guide Pratique Correspondant), kojeg je izdalo francusko tijelo za zaštitu podataka, the CNIL, in 2011, dostupno na: https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf U Italiji, nacionalno tijelo za zaštitu podataka, Garante del Privacy, izdalo je zbirku Često postavljanih pitanja (FAQs) o SZP-ovima, dostupno na: https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (FAQs for DPOs in the private sector) https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (FAQs for DPOs in the public sector) U Poljskoj, nacionalno tijelo nadležno za zaštitu podataka, Urząd Ochrony Danych Osobowych (UODO), izdaje korisne savjete i preporuke za primjenu GDPR-a na njihovoj web stranici, koje su dijelom posvećene posebno DPO-ima: https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych. Prije stupanja na snagu GDPR-a, poljsko nadležno tijelo održavalo je ABI web stranicu za ono što se prije nazivalo, Administratori informacijske sigurnosti. Stranica je sadržavala informacije korisne također i za priremanje budućih SZP-ova za njihovu funkciju, vidi: https://abi.giodo.gov.pl/. Kroz navedenu uslugu, budući DPO-i mogli su postaviti svoja pitanja i izložiti sugestije vezano za primjenu i tumačenje zakonskih odredbi o zaštiti osobnih podataka. U UK-u, nacionalno tijelo za zaštitu podataka, the Information Commissioner (koje se obično naziva the ICO, što je skraćenica za Information Commissioner's Office), daje smjernice na svojim mrežnim stranicama koja u biti održavaju (i referiraju se na) smjernice WP29, vidi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

243 Primjerice, švedski TZP je najavio da će kontrolirati jesu li organizacije u sektorima bankarstva, zdravstvene zaštite i osiguranja imenovale SZP-ove.Vidjetihttps://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-gdpr/**Nizozemski**TZPsličnojenaglasiousvojemplanu za 2018. – 2019. da će, *posebice u odnosu na javna tijela,* provjeravati: "*sukladnost s obvezom vođenja evidencije postupaka obrade, obvezom imenovanja SZP-a, i način na koji organizacija postavlja SZP i omogućava mu da ispunjava svoje zadaće koje on mora ispunjavati sukladno GDPR-u*", vidjeti: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegev ens_2018-2019.pdf (str. 7, pod naslovom "*Overheid*" (javno tijelo) (naš prijevod).

MEĐUNARODNA I NACIONALNA UDRUŽENJA SLUŽBENIKA ZA ZAŠTITU PODATAKA:

Međunarodna udruženja:

Globalna:
International Association of Privacy Professionals (IAPP):
https://iapp.org/certify/cipp/

Europska:
Network of Data Protection Officers of the EU Institutions and Bodies:
https://ENZP.europa.eu/data-protection/eu-institutions-dpo_en

Confederation of European Data Protection Organisations, CEDPO
http://www.cedpo.eu/

Nacionalna udruženja:
(Oni označeni (*) članovi su CESZP-a)

Francuska:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/account-ability-andgovernance/data-protection-officers/

*Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:**
https://www.afcdp.net/

Irska:
Association of Data Protection Officers, ADPO:*
https://www.dpo.ie/

Italija:
Associazone Data Protection Officer, ASSO DPO:*
http://www.assodpo.it/en/home_en/

Nizozemska:
Nederlands Genootschap voor Functionarissen Gegevensbescherming, NGFG:*
https://www.ngfg.nl/

Poljska:
Stowarzyszenie Administratorów Bezpieczeństwa Informacji, SABI:* http://www.sabi.org.pl/

Španjolska:
Asociación Profesional Española de Privacidad, APEP:*
http://www.apep.es/

UK:
National Association of Data Protection & Freedom of Information Officers, NADPO:
https://nadpo.co.uk/

Njemački i austrijski članovi CESZP-a, odnosno the Gesellschaft für Datenschutz und Datensicherheit e.V., DGG* (osnovano 1977. g.) i Arge Daten*, imaju šire članstvo koje uključuje i druge osim SZP-ova, ali su oba članovi CESZP-a:
https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

2.5.2 Obveza imenovanja Službenika za zaštitu podataka za javna tijela[244]

Imenovanje SZP-a je obvezno za sva javna tijela ili tijela koja obrađuju osobne podatke na koje se primjenjuje GDPR (čl. 37(1)(a)).[247] Iako je to načelno ostavljeno državama članicama, RS29 s pravom zauzima širi pogled na ovaj zahtjev:[245]

"Tijelo javne vlasti ili javno tijelo"

GDPR ne definira što predstavlja "tijelo javne vlasti ili javno tijelo". RS29 smatra da se takav pojam treba odrediti nacionalnim pravom. Shodno tome, tijela javne vlasti ili javna tijela uključuju državne, regionalne i lokalne vlasti, ali koncept, prema važećim nacionalnim pravima, tipično također uključuje i čitav niz drugih tijela za koje je mjerodavno javno pravo.[246] U tim slučajevima, imenovanje SZP-a je obvezno.

Međutim, obveza imenovanja SZP-a zapravo se proširuje i izvan ove čisto formalne kategorije.

Osobe iz privatnog sektora koje provode "zadaće od javnog interesa" ili koje "izvršavaju službene ovlasti"

RS29 naglašava, uz reference na posebnu pravnu osnovu za obradu iz čl. 6(1)(e) GDPR-a, da (neovisno o ograničenjima obveza imenovanja SZP-a za "isključivo" privatne osobe)[250], SZP treba uvijek biti imenovan od strane voditelja obrade iz privatnog sektora, koji provode "zadaće … od javnog interesa" ili koji "izvršavaju službene ovlasti", čak i ako formalno nisu "javna tijela" u smislu domaćeg nacionalnog prava, jer će u takvim aktivnostima njihova uloga biti slična ulozi javnih vlasti:[247]

Javna zadaća može se obavljati, a javna vlast se može izvršavati ne samo od strane javnih tijela ili tijela javnih vlasti, već također i od strane drugih fizičkih ili pravnih osoba za koje je mjerodavno javno ili privatno pravo, u sektorima kao što su, sukladno nacionalnim zakonodavstvima svake države članice, usluge javnog prijevoza, vodoopskrba i opskrba

(članak 37(1)(b) i (c) GDPR-a)

Ovi zahtjevi su donekle opisani u Smjernicama RS29 o SZP-ovima. Za potrebe ovog Priručnika, dostatno je primijetiti da će u praksi za većinu društava bilo koje veličine biti od pomoći imenovati SZP kako bi ispunili svoje zahtjeve "pouzdanosti"[odgovornosti]/"obveza dokazivanja usklađenosti", o čemu se govori pod toč. 2.2. [247] Jedina iznimka u ovom smislu odnosi se na "sud[ove] koji djeluju u okviru svoje sudske nadležnosti" (čl. 37(1)(a) GDPR-a). Međutim, kako RS29 naglašava u svojim Smjernicama o SZP-ovima (ranija bilješka), to ne znači da ne moraju biti u sukladnosti s Uredbom – upravo suprotno: i oni moraju postupati sukladno Uredbi. A u pogledu obrade od strane sudova osim u njihovoj sudskoj nadležnosti, i za njih postoji obveza imenovanja SZP-a.

244 Osim u odnosu na privatne osobe koje provode "javne zadaće" ili "provode zadaće od javnog interesa" – kako se objašnjava u tekstu – obveza imenovanja SZP-a za "isključivo" privatna (komercijalna) trgovačka društva nije pitanje raspravljeno u ovom Priručniku. Dostatno je primijetiti da Uredba za takve pravne osobe u načelu propisuje da je imenovanje SZP-a obvezatno samo u sljedećim slučajevima:

- kada se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri; ili
- osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. [tj. tzv. "osjetljivi podaci"] i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.

245 Smjernice RS29 o SZP-ovima, (bilješka (fusnota) 11, prethodno u tekstu) str. 6.

246 Vidjeti, npr. definiciju "tijelo javnog sektora" i "tijelo uređeno javnim pravom" u članku 2(1) i (2) iz Direktive 2003/98/EZ Europskog parlamenta i Vijeća od 17. studenog 2003. o ponovnoj uporabi informacija javnog sektora, SL L 345, 31.12.2003, str. 90ff. [izvorna bilješka (fusnota)] Hrvatski tekst ove direktive, dostupan je ovdje: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32003L0098&from=HR [250] Vidi bilješku (fusnotu) 17, prethodno u tekstu.

247 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), str. 6, uz dodano podebljavanje teksta. Izrazi koje koriste RS29, "javna zadaća" i "javno tijelo" isključivo su lingvističko pitanje: u smjernicama, ovi se izrazi odnose na "zadaće od javnog interesa" i "izvršavanje službenih ovlasti" spomenuto u čl. 6(1)(e) GDPR-a.

Ovaj se Priručnik ne bavi SZP-ovima za tijela koja provode obradu koja je u cijelosti izvan polja primjene EU prava, kao što su nacionalne agencije za sigurnost.

električnom energijom, cestovna infrastruktura, javna usluga [radio ili tv] emitiranja, stanovanje u državnim stanovima ili disciplinarna tijela za regulirane profesije.

U tim slučajevima, ispitanici mogu biti u vrlo sličnoj situaciji onoj kada se njihovi podaci obrađuju od strane javnih tijela ili tijela s javnim ovlastima. Posebice, podaci se mogu obrađivati za slične svrhe, a pojedinci često imaju slično malo ili uopće nemaju izbora o tome hoće li i na koji način njihovi podaci biti obrađivani te stoga mogu trebati dodatnu zaštitu koju imenovanje SZP-a može pružiti.

Premda ne postoji obveza u takvim slučajevima, RS29 preporučuje, kao dobru praksu, da privatne organizacije koje provode javne zadaće ili izvršavaju službene ovlasti imenuju SZP. Aktivnost takvog SZP-a obuhvaća sve aktivnosti obrade koje se provode, uključujući i one koje nisu vezane za provođenje javne zadaće ili izvršavanje službene dužnosti (npr. upravljanje bazom podataka zaposlenika).

Uz primjere koje spominje RS29, moglo bi se dodati upravljanje zatvorima ili drugim državnim institucijama ili pružanje drugih usluga (kao što je deportacija imigranata koji nezakonito borave u državi), od strane privatnih tijela. U svim tim slučajevima, privatna tijela učinkovito djeluju kao produžena ruka države – i u svim takvim slučajevima, dotična društva bi trebala imenovati SZP. Države članice mogu dalje razjasniti ovo pitanje u svojem nacionalnom pravu, te nametnuti obvezu imenovanja SZP-a određenim voditeljima obrade ili vrstama voditelja obrade, osim onih koji su javna tijela ili tijela s javnim ovlastima (usp. čl. 37(4)).

PRIMJER:

U **Italiji**, nacionalno tijelo za zaštitu podataka, Garante, zauzima stav da se treba smatrati kako sve osobe koje podliježu polju primjene odlomaka 18. do 22. talijanskog Zakonika o zaštiti podataka moraju imenovati SZP. Odlomci 18. do 22. Zakonika navode opća pravila koja se primjenjuju na obradu koju provode javna tijela – kao što su državna upravna tijela, neprofitna javna tijela na nacionalnoj, regionalnoj i lokalnoj razini, regije, lokalne vlasti, sveučilišta, trgovačke komore, agencije za zdravstvenu zaštitu, neovisna nadzorna tijela itd.

Garante također drži da kad god privatna osoba obavlja javne funkcije – npr. na temelju licence ili koncesije – imenovanje SZP-a se snažno preporučuje, premda nije obvezno. Oni nadalje dodaju, s pozivom na Smjernice RS29 o SZP-ovima, da ako se SZP imenuje dobrovoljno, primjenjuju se isti zahtjevi i uvjeti kao i u slučaju da je SZP bio imenovan po načelu obvezatnosti – u smislu kriterija za imenovanje SZP-a, radnog mjesta i zadaća.

SZP-OVI ZA IZVRŠITELJE OBRADE

Kako RS29 ističe, članak iz GDPR-a koji nameće obvezu imenovanja SZP-a u određenim slučajevima (čl. 37), kako je prethodno izloženo za javni sektor, vrijedi i za izvršitelje i za voditelje obrade.[248] Nadalje se dodaje:[249]

Ovisno o tome tko ispunjava kriterije za obvezno imenovanje, u nekim slučajevima samo voditelj obrade ili samo izvršitelj obrade, a u drugim slučajevima i voditelj i izvršitelj obrade trebaju imenovati SZP-a (koji bi potom trebao surađivati međusobno s njima).

248 RS29 Smjernice o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), u odlomku 2.2, SZP *of the processor* (SZP *izvršitelja obrade)*, na str. 9.
249 *Idem*. RS29 navodi neke primjere, uzete iz privatnog sektora, koji se fokusiraju na ograničenja obveze imenovanja SZP-a za taj sektor; to stoga nije posebno korisno u ovom Priručniku.

Važno je naglasiti da čak i ako izvršitelj obrade ispunjava kriterije za obvezno imenovanje, njegov izvršitelj ne mora nužno imenovati SZP-a. Ovo bi, svejedno, bila dobra praksa.

Za javni sektor, u kojem ionako sva nadležna tijela moraju svakako imenovati SZP-a (kako se prethodno obrazlaže), ovo se ne mora činiti bitnim pitanjem. Međutim, u svjetlu posljednjeg komentara RS29, ako bi javno tijelo za neke aktivnosti obrade uzelo podizvođača koji je privatna pravna osoba (npr. računovodstvo ili anketiranje), bilo bi barem preporučljivo odabrati izvršitelja koji i sam već ima SZP-a, ili pak zatražiti od izvršitelja koji još nema SZP-a da ga imenuje.

U mjeri u kojoj javna tijela koja surađuju mogu također s vremena na vrijeme djelovati kao izvršitelji obrade jedni za druge, to bi se štoviše trebalo odražavati i u pisanoj evidenciji o njihovim aranžmanima, što je opisano pod podnaslovom i detaljnije obrazloženo u 3. dijelu, u odlomku 3.1.

SZP-OVI ZA JAVNA TIJELA VEĆEG KAPACITETA ILI GRUPE TIJELA

Uz "digitalnu transformaciju", osobni podaci se sve više obrađuju u iznimno složenim okruženjima i tehničkim strukturama, u kojima različiti dionici blisko surađuju, te imaju zajedničke ili povezane uloge u odnosu na različite postupke obrade – uključujući i u odnosu na građane. Ovo je također slučaj u javnom sektoru, koji doista ima svoje složenosti u smislu stupnja autonomije kojeg različite agencije mogu imati unutar šireg ustavnog ili upravnopravnog okvira. Kako se dalje pojašnjava u trećem dijelu, u odlomku 3.1, jedna od prvih zadaća bilo kojeg novoimenovanog SZP-a mora biti "opseg" konteksta za obradu osobnih podataka u kojima će imati nadležnost nadgledati i/ili savjetovati. Dio ovog posla bit će razjasniti, u pogledu takvih složenih konteksta, koji je točno položaj različitih pravnih osoba koje su dio tog konteksta te sklopiti i zabilježiti odgovarajuće aranžmane.

U tom smislu, treba primijetiti da GDPR izrijekom propisuje (kao što je to činila i Direktiva o zaštiti podataka iz 1995. g.) da "kada su svrhe i sredstva … obrade utvrđeni pravom Unije ili pravom države članice" (što će obično biti slučaj za javne vlasti) "voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice" (čl. 4(7)). Često će imati smisla, u takvim slučajevima, imenovati SZP-a za svaku obradu obuhvaćenu takvim određivanjem u uredima pravne osobe koja je određena kao voditelj obrade. Doista, pravo koje određuje voditelja obrade može samo po sebi navedeno pojasniti.

Ako navedeno nije određeno pravom, moguće je da pitanje treba riješiti nadležno ministarstvo/ministar, visokopozicionirani službenik ili to trebaju riješiti sama javna tijela između sebe. Ovo bi trebalo dovesti do jasnih aranžmana za odnosne odgovornosti i kompetencije različitih SZP-ova u različitim tijelima koja su dio kompleksa. Dio ovoga uključuje odluku o tome gdje imenovati SZP-a ili nekolicinu SZP-ova. Aranžmani bi također trebali pokrivati poveznice i aranžmane između različitih SZP-ova u operativno povezanim tijelima.

Neka tijela javne vlasti većeg kapaciteta (ili državna ministarstva ili viši službenici takvih tijela) mogu odlučiti imenovati nekoliko SZP-ova za svaki od njegovih sastavnih dijelova – pod uvjetom da to odražava stvarnu raspodjelu ovlasti odlučivanja između pojedinih odjela ili jedinica tih javnih tijela velikog kapaciteta. Ili pak oni mogu odlučiti imenovati jednog SZP-a za cijelo tijelo, koji surađuje s imenovanim osobama u tim dijelovima cijelog tijela većeg kapaciteta. U potonjem slučaju, slijedi iz komentara koje je napisao RS29 u kontekstu imenovanja SZP-ova na temelju ugovora o djelu (o čemu se govori pod sljedećim podnaslovom), da takve imenovane osobe u odjelima ili odvojenim jedinicama velike organizacije trebaju s jedne strane ispunjavati uvjete za SZP-ove, posebice uvjet da ne postoji sukob interesa, a s druge strane – treba im se pružiti ista zaštita kao pravom SZP-u, a ne da budu penalizirani za provođenje funkcija vezanih za ulogu SZP-a.[250]

Suprotno tome, GDPR izrijekom dopušta grupama (formalno odvojenih) manjih javnih tijela – kao što su lokalne vlasti (Fr: *communes*) – da odluče (ili dobiju uputu) zajednički imenovati SZP:

250 Usp. Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), pod točkom 2.4, posljednja natuknica, na str. 12.

> Ako je voditelj obrade ili izvršitelj obrade tijelo javne vlasti ili javno tijelo, za nekoliko takvih vlasti ili tijela može se imenovati jedan službenik za zaštitu podataka, uzimajući u obzir njihovu organizacijsku strukturu i veličinu (čl. 37(3)).

Takav glavni ili zajednički SZP bi mogao biti ili službenik jednog od tih tijela ili bi se moglo zajednički odlučiti da se angažira vanjski SZP, na osnovi ugovora o djelu (kako se objašnjava pod sljedećim podnaslovom). Ako se imenuje jedan glavni (interni /*in-house*/ ili vanjski) SZP, druga (manja) tijela trebala bi i dalje odrediti jednog od zaposlenika odgovornog za suradnju s glavnim (zajedničkim) SZP-om – i u tom slučaju vrijedi isto što je upravo bilo navedeno u pogledu većih tijela: imenovane osobe trebaju ispunjavati uvjete za SZP-a, i treba im biti pružena slična zaštita kao i pravom SZP-u.

VANJSKI SZP-OVI

Kako je već ranije navedeno pod prethodnim podnaslovom, javna tijela (i privatna trgovačka društva) ne moraju predvidjeti *in-house* radno mjesto za SZP-a, a pogotovo ne radno mjesto na puno radno vrijeme (premda mnoga veća tijela vjerojatno odabiru učiniti upravo to, ako to već i nisu učinili). Umjesto toga:

> "[s]lužbenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade ili obavljati zadaće na temelju ugovora o djelu" (čl. 37(6)).

U Njemačkoj, odakle potječe ideja o SZP-ovima,[251] odvjetnički uredi ili drugi neovisni stručnjaci nude funkcije SZP-a na ovaj način. Štoviše, "udruženja i druga tijela koji predstavljaju kategoriju voditelja obrade ili izvršitelja obrade" mogu, čini se, slično pružati funkcije SZP-a svojim članovima, te u tom smislu nastupati za račun svih tih članova (usp. čl. 37(4)). Ovo bi posebno bilo korisno za mala poduzeća. Velik broj velikih konzultantskih kuća i odvjetničkih

ureda također nudi SZP podršku "na temelju ugovora o djelu", a postojat će i neka manja poduzeća, posebno ona specijalizirana za ICT poslove, koja će nuditi ovu uslugu na toj osnovi.

Međutim, takvi vanjski SZP-ovi ne bi trebali biti previše udaljeni od tijela kojima pružaju usluge: jer kao što je objašnjeno u sljedećem dijelu ovog Priručnika, SZP-ovi moraju posjedovati cjelovito i suštinsko razumijevanje tih tijela i njihovih postupaka obrade podataka. Oni također moraju biti potpuno i lako dostupni – osoblju u dotičnim tijelima, kao i ispitanicima i tijelima za zaštitu podataka (nadzorna tijela). Njihovi kontakt podaci trebaju biti jasno navedeni na mrežnim stranicama nadležnih tijela i u odgovarajućim brošurama itd.

Francusko tijelo za zaštitu podataka, CNIL, smatra da bi SZP trebao "po mogućnosti" biti član osoblja organizacije voditelja obrade, ali prihvaća činjenicu da ovo neće baš uvijek biti moguće za manja i srednja poduzeća.[252]

U javnom sektoru, često može biti pogodno imati SZP-a iz određenog predmetnog sektora – npr. kako se obrazlaže pod prethodnim podnaslovom, glavni SZP za javno tijelo većeg kapaciteta ili zajednički SZP za grupu manjih tijela pridružen jednome od njih – bolja je to opcija nego imati vanjskog SZP-a koji dolazi iz tvrtke iz privatnog sektora, ali ovo će ovisiti o kulturi i praksi u dotičnoj državi.

251 Vidjeti tekst pod točkom 2.3.1, prethodno u tekstu.
252 CNIL, *Guide Pratique Correspondant* (bilješka (fusnota) 63, prethodno u tekstu), str. 6.

2.5.3 Kvalifikacije, kvalitete i radno mjesto SZP-a

TRAŽENA STRUČNOST

Uredba propisuje kako slijedi:

> Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito **stručnog znanja o pravu i praksama u području zaštite podataka** te **sposobnosti izvršavanja zadaća** iz članka 39 [kako je objašnjeno u nastavku, pod točkom 2.3.4] (čl. 37(5), dodatno naglašeno)

Vezano za prvi uvjet – stručno znanje – dokument koji sadrži "profesionalne standarde" SZP-ova iz EU institucija navodi potrebu za udovoljavanjem sljedećih uvjeta:[253]

(a) Stručnost u području EU prava o privatnosti i zaštiti podataka, posebice članka 16 Ugovora o funkcioniranju Europske unije, članka 8 Povelje Europske unije o temeljnim pravima, Uredbe (EZ) 45/2001 i drugih relevantnih zakonskih instrumenata o zaštiti podataka, kao i stručnost u području IT-a i IT sigurnosti; i

(b) Dobro poznavanje načina na koji funkcionira institucija [u kojoj je SZP imenovan] i njenih postupaka obrade osobnih podataka, kao i sposobnost tumačiti relevantna pravila o zaštiti podataka u tom kontekstu.

Tehničko poznavanje IT sustava treba posebno biti naglašeno. Kako navodi **francusko** tijelo za zaštitu podataka, CNIL:[254]

> U odnosu na informatiku, potrebno je dobro poznavanje terminologije, [IT] prakse i različitih oblika obrade podataka. SZP bi trebao imati znanje o, primjerice, upravljanju podacima i sustavima korištenja podataka, vrstama softvera, sustavima pohrane datoteka i podataka, kao i o potrebi čuvanja povjerljivosti i politici sigurnosti (enkripcija podataka, elektronički potpisi, biometrija …). Ovo znanje bi trebalo omogućiti [SZP-u] nadzirati uvođenje IT projekata i pružanje korisnih savjeta voditelju obrade koji je odgovoran za obradu.

Uvodna izjava 97 GDPR-a također naglašava da:

> Nužna razina stručnog znanja trebala bi se utvrditi posebno u odnosu na postupke obrade podataka koji se provode te na zaštitu koju za obrađene osobne podatke zahtijeva voditelj obrade ili izvršitelj obrade.

Drugim riječima, priroda traženog "stručnog znanja" i "sposobnosti" može varirati, ovisno o djelatnostima voditelja obrade: SZP za poreznu upravu će trebati posjedovati drugačiju stručnost negoli onaj koji radi za tijelo u sektoru obrazovanja ili zdravstvene skrbi. ENZP na ovu temu govori o potrebi "**bliskosti**" (misli se: bliskosti SZP-a i tijela kojeg opslužuje):[255]

> SZP ima ključnu ulogu unutar institucije/tijela: SZP-ovi su [tj., trebaju biti] upoznati s problemima tijela u kojem rade (*ideja bliskosti*) i, obzirom na njihov status, igraju ključnu ulogu u davanju savjeta i pružanju pomoći kod rješavanja pitanja koja se tiču zaštite podataka [što znači: koja su karakteristična za dotično tijelo].

253 Network of Data Protection Officers of the EU Institutions and Bodies (Mreža SZP-ova EU institucija i tijela), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Profesionalni standardi za SZP-ove EU institucija i tijela koji rade sukladno Uredbi (EZ) 45/2001) (bilješka 13, iznad), str. 3-4.
254 CNIL, *Guide Pratique Correspondant* (bilješka 63, iznad), str. 8 (naš prijevod)
255 EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (bilješka 12, iznad), str. 5, dodano isticanje.

Kako se navodi u Smjernicama RS29 o SZP-ovima:[256]

> SZP bi također trebao imati dostatno razumijevanje postupaka obrade koji se provode [u dotičnom sektoru i organizaciji], kao i informacijskih sustava te potreba za sigurnosti podataka i zaštiti podataka samog voditelja obrade.
>
> U slučaju javnog tijela ili tijela s javnim ovlastima, SZP bi uvijek trebao dobro poznavati [interna] administrativna pravila i procedure organizacije.

Ovome bi se moglo dodati: također je potrebno poznavanje zakona, pravila i procedura sukladno kojima dotično javno tijelo funkcionira (npr. Porezni zakon ili Zakon o obrazovanju, itd.), kao i upravno pravo i postupak općenito.

S druge strane, kako je opisano u nastavku pod naslovima "*Sukobi interesa*" i "*Radno mjesto unutar organizacije*", imenovanje osobe koja je već u postojećem osoblju javnog tijela može izazvati probleme, posebno ako je imenovani imenovan na nepuno radno vrijeme, a zadrži ostale funkcije unutar dotičnog tijela.

Stručno znanje zakona i praksi koji se tiču zaštite podataka općenito može se dokazati tečajevima za osposobljavanje i internetskim (*online*) ili drugim tečajevima ili edukacijama, itd. koje je dotična osoba završila – kao što su oni koje nudi "T4DATA" program u kontekstu kojega je ovaj Priručnik napisan. Ali također su široko dostupne i mnoge druge edukacije, različitih stupnjeva i kvalitete kako se navodi u nastavku.

FORMALNA EDUKACIJA I CERTIFIKACIJA

U vrijeme pisanja ovog dokumenta (prosinac 2018.) u jednoj državi članici EU-a, Španjolskoj, poduzimani su koraci ka stvaranju formalnog sustava certificiranja SZP-ova, ali to još nije u funkciji.[257] Štoviše, ovaj certifikacijski sustav za SZP-ove (i neke druge koji se razmatraju) temelji se na ISO 17024, tj. na shemi certificiranja za pojedince i profesionalce; kao takvi, oni ne ispunjavaju zahtjeve norme ISO 17065 koja je shema navedena u konceptu certifikacije pod GDPR-om (certificiranje usluga, proizvoda, eventualno sustava upravljanja). Dakle, certifikati vezani uz SZP-ove se razlikuju od "certifikata" iz članka 42 GDPR-a. Oni su pohvalni, ali nisu sukladni s GDPR-om.

U Francuskoj je TZP, CNIL, 11. listopada 2018. godine izdalo dva *référentialsa* (engl.: specifikacije) koji se odnose na certifikaciju SZP-ova, a objavljeni su u nacionalnom Službenom listu. Jedan se odnosi na certifikaciju koja se odnosi na kompetencije SZP-a, a druga na određivanje nadležnosti SZP-a te na akreditacijsku organizaciju ovlaštenu za certificiranje SZP-a.[258]

U doba pisanja ovog priručnika (kolovoz 2018.), u jednoj državi članici EU-a, Španjolskoj, poduzeti su koraci prema stvaranju formalne sheme certificiranja za SZP-ove, ali to još nije u operativnoj fazi.

U Njemačkoj se nude različiti tečajevi i seminari kako bi se osposobile osobe, a neki od tih rezultiraju nekim oblikom certifikacije,[259] no usprkos tome što je ta institucija već dugo poznata u toj državi, ipak ne postoji zakonski utemeljena, službeno priznata shema.

---

256 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), str. 11.

257 Španjolsko nacionalno tijelo za zaštitu podataka, Agencia Española de Protección de Dato (AEPD) uspostavilo je sustav certificiranja za službenike za zaštitu podataka (Esquema de Certificateón de Delegados de Protección de Datos de la Agencia Española de Protección de Datos) prema kojoj nacionalna španjolska agencija za akreditaciju (la Entidad Nacional de Acreditación - ENAC) može akreditirati tijela za certificiranje (Entidades de Certificación), kojima je dopušteno izdavanje odgovarajućih certifikata, na temelju kriterija koje je razvio TZP (AEDP) i službeni ispit, vidi: https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (verzija 1.3, 13. lipnja 2018.) Međutim, takva certifikacijska tijela još nisu akreditirana te stoga još nisu izdani certifikati SZP-a. Vidi također kratku, općenitiju raspravu o shemama certificiranja u gornjoj točki 2.1 https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

258 Pogledati: https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

259 Usp., npr.: https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragternach-bdsg-mit-dekra.html

Nekoliko međunarodnih i nacionalnih udruženja SZP-ova, navedenih ranije, također nude specijalizirane obuke – ali opet, bez zakonske podloge.[260]

Mnogi od ovih tečajeva ili seminara osposobljavanja ciljano su usmjereni na osiguravanje polaznicima stručnosti oko GDPR-a i davanje smjernica o zadaćama dodijeljenima SZP-ovima prema GDPR-u. Ali GDPR (kao i njemački i drugi nacionalni zakoni) ne predviđa detaljnije kriterije ili sheme certificiranja. Moguće je da će u budućnosti, osim Španjolske, i druge države članice također pružati takve formalne, službeno priznate sheme ili bi pak Europski odbor za zaštitu podataka mogao (vjerojatno neformalno) podržati neke od tih.[261] Ali dok se to ne dogodi, parametri i dalje ostaju prilično otvoreni. Kako navodi **talijansko** tijelo za zaštitu podataka, *Garante*:[262]

> Kao i u slučaju s tzv. "nereguliranim profesijama", razvijene su zakonski zaštićene sheme da bi se certificirale, na dobrovoljnoj bazi, profesionalne vještine i kompetencije. Takve sheme vodi nekoliko certifikacijskih tijela. Certifikacije ove vrste – koje ne podliježu opsegu odredbe iz članka 42. GDPR-a – ponekad se izdaju nakon pohađanja edukacije i/ili tečajeva za verifikaciju učenja.
>
> Premda predstavljaju vrijedan alat koji, slično drugim atestiranjima, može pružiti dokaz o tome da određeni stručnjak posjeduje barem osnovno znanje o važećim pravilima, takve certifikacije nisu identične, *per se*, 'kvalifikacijama' koje omogućavaju prepuštanje zadaća vezanih za posao SZP-a i ne mogu zamijeniti obvezu javnih upravnih tijela da procijene uvjete koje SZP mora zadovoljavati s obzirom na zadaće i obveze navedene u članku 39. GDPR-a.

Kako je to izrazilo Udruženje europskih organizacija za zaštitu podataka (the Confederation of European Data Protection Organisations, CESZP):[263]

> Kandidati će vam vjerojatno pokazati mnoge certifikate (potvrde) i diplome koje su sakupili kroz godine kako bi pokazali koliko su kvalificirani. Ali kako odrediti koje su doista vrijedne, a koje nisu? Prije svega, trebate provjeriti vjerodostojnost osobe koja vodi edukaciju i certifikaciju. Ako je to dobro poznata akreditirana pan-EU ili nacionalna organizacija (u nekim državama čak i tijela za zaštitu podataka izdaju certifikate), možete se ipak malo opustiti. Također, saznajte program tih edukacijskih tečajeva.
>
> Jednodnevno događanje ili certifikacije koje su uglavnom rezultat uplate i vrlo jednostavnog ispita neće rezultirati time da netko postane pouzdan SZP.

Svi različiti dokumenti sa smjernicama također naglašavaju potrebu da organizacije osiguraju da njihov SZP može nastaviti održavati i ojačavati svoju stručnost i nakon svojeg imenovanja, i to pohađanjem odgovarajućih tečajeva i seminara. Ovo doista također propisuje i GDPR (vidjeti završetak odredbe iz čl. 38(2)). Kako je to sročio RS29:[264]

> SZP-ovima bi trebalo dati mogućnost da ostanu u toku s novostima iz domene zaštite podataka. Cilj bi trebao biti kontinuirano povećavati stupanj stručnosti SZP-ova i trebalo bi ih poticati da sudjeluju na edukacijskim tečajevima o zaštiti podataka i drugim oblicima profesionalnog razvoja, kao što je sudjelovanje na forumima za privatnost, radionicama itd.

260 Dokument Standardi SZP-a iz EU institucija preporučuje sheme Međunarodne institucije stručnjaka za pitanja privatnosti (IAPP). IAPP nudi certifikacije specifične za pojedine regije, uključujući i onu koja je europski usmjerena koje posebice obuhvaća GDPR. Vidjeti: https://iapp.org/certify/cippe/ Mreža SZP-ova EU institucija i tijela, profesionalni standardi Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (bilješka (fusnota) 13, prethodno), str. 5. Dokument SZP-ova iz EU institucija također spominje upravljanje IT sigurnosti i certifikacijske revizije, ali oni su općenitiji i nisu specifično usmjereni na zaštitu podataka.

261 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), samo navodi da "je također od pomoći ako nadzorna tijela promoviraju odgovarajuće i redovito osposobljavanje za SZP-ove." (str. 11). [266] *Garante del Privacy*, FAQs on DPOs (Česta pitanja o SZP-ovima) (bilješka (fusnota) 63, prethodno u tekstu), odl. 3.

262 Garante del Privacy, FAQs on DPOs (Česta pitanja o DPO-ovima) (bilješka (fusnota) 63, ranije u tekstu), odl. 3.

263 CEDPO, Choosing the best candidate as your Data Protection Officer (SZP) – Practical guidelines for organisations (Odabir najboljeg kandidata za vašeg Službenika za zaštitu podataka (SZP) - Praktične smjernice za organizacije (bilješka (fusnota) 8, prethodno u tekstu), str. 2.

264 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), str. 14.

Francusko tijelo za zaštitu podataka, CNIL, vrlo korisno pruža poseban "**extranet**" za registrirane SZP-ove, koji je dostupan jedino njima korištenjem korisničkog imena i lozinke, a na kojem mogu pronaći pravne tekstove (zakone, uredbe itd.) i podatke o tečajevima i informacije, uključujući informacije o novim izvješćima ili smjernicama koje izdaje CNIL, kao i o drugim pravnim i praktičnim novostima te im omogućava razmjenu stajališta i vođenje diskusija.[265]

ISKUSTVO

Smjernice RS29 o SZP-ovima ne dotiču se pitanja koliko (vremenski) iskustvo treba imati SZP. Međutim, Mreža europskih institucionalnih SZP-ova preporučuje da takvi SZP-ovi trebaju imati sljedeće iskustvo/profesionalnu zrelost:[266] najmanje 3 godine relevantnog iskustva [vidjeti u nastavku] da bi se obavljala dužnost SZP-a u tijelu u kojem zaštita podataka nije vezana za osnovnu djelatnost [*idem*] (i stoga su postupci obrade osobnih podataka uglavnom administrativni); i najmanje 7 godina relevantnog iskustva da bi se obavljala dužnost SZP-a u EU instituciji ili onim tijelima EU-a gdje je zaštita podataka vezana za osnovnu djelatnost ili gdje zaštita podataka ima veliku važnost u postupcima obrade osobnih podataka.

U bilješci (fusnoti) dodaju sljedeće:

> Relevantno iskustvo uključuje iskustvo u provedbi zahtjeva zaštite podataka i iskustvo unutar institucije/organizacije koja imenuje SZP, koje rezultira poznavanjem načina kako ista funkcionira. Ako ne postoji dostatan uvjet dužine iskustva, tijelo/institucija koja imenuje SZP treba biti spremna dodijeliti više vremena SZP-u za edukaciju i rad na zadaćama zaštite podataka.

O pitanju je li obrada osobnih podataka "vezana za osnovnu djelatnost" dotične organizacije, relevantne su RS29 smjernice o značenju slične fraze iz GDPR-a ("osnovne djelatnosti voditelja obrade ili izvršitelja obrade"):[267]

> 'Osnovne djelatnosti' mogu se smatrati ključnim djelatnostima potrebnima da bi se postigli ciljevi voditelja obrade ili izvršitelja obrade.

Fraza "odgovarajuće iskustvo" ne bi se trebala tumačiti kao specifično iskustvo na mjestu SZP-a – to može biti iskustvo izrade i primjene pravila (politika) u relevantnoj organizaciji (ili sličnoj organizaciji) ili u relevantnim područjima, kao što su IT, razvoj proizvoda itd. Dostatno je naglasiti da radno mjesto ne bi trebalo dodijeliti relativno mladoj, neiskusnoj osobi ni osobi koja nije upoznata s određenom organizacijom ili tom vrstom organizacije.

OSOBNE KARAKTERISTIKE I KVALITETE

ENZP, udruženje EU-ovih institucionalnih SZP-ova i CEDPO svi ispravno primjećuju da SZP mora imati posebne osobne kvalitete. Ta osoba je u delikatnom položaju: mora biti voljna reći "ne" i nadređenima u rijetkim slučajevima, ali češće mora biti u stanju pomoći u iznalaženju rješenja, koje je prihvatljivo i za organizaciju, a istovremeno je potpuno sukladno pravu (i ako ništa drugo, ojačavanju privatnosti). Kako je to naveo RS29 u Smjernicama:[268]

265 CNIL, *Guide Pratique Correspondant* (bilješka (fusnota 228, prethodno u tekstu), odlomak 4.
266 Network of Data Protection Officers of the EU Institutions and Bodies (Mreža SZP-ova EU institucija i tijela), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Profesionalni standardi za SZP-ove u EU institucijama i tijelima koji rade prema Uredbi (EZ) 45/2001) (bilješka (fusnota) 13, prethodno u tekstu), str. 4.
267 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), str. 6.
268 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), str. 11.

> Osobne kvalitete trebaju uključivati primjerice integritet i visoku profesionalnu etiku; prvenstvena briga SZP-a trebala bi biti omogućavati postizanje sukladnosti s GDPR-om. SZP igra glavnu ulogu u usvajanju kulture zaštite podataka unutar organizacije i pomaže u provedbi ključnih elemenata GDPR-a …

SZP-ovi zaposleni u EU institucijama naglašavaju potrebu za sljedećim "osobnim" i "interpersonalnim" vještinama:[269]

> Osobne vještine: integritet, inicijativa, organizacija, ustrajnost, diskrecija, sposobnost afirmirati se i u teškim okolnostima, zanimanje za zaštitu podataka i motivacija biti SZP.
>
> Interpersonalne vještine: komunikativnost, sposobnost pregovaranja, rješavanje sporova, sposobnost graditi radne odnose.

Osim toga, oni navode:[270]

> Ispravno obavljanje zadaća SZP-a često zahtijeva čvrst i nepokolebljiv stav i s voditeljima obrade koji su visoko pozicionirani u organizaciji, što se moguće percipira, u najboljem slučaju, kao birokratsko ponašanje, ili, još gore, kao neugodno "izazivanje problema". Stoga, SZP mora biti u stanju oduprijeti se pritiscima koji prate ovu poziciju.

CEDPO dodaje:[271]

> SZP se mora suočiti s brojnim izazovima i s različitim interesima koji su uključeni. Zbog toga bi SZP trebao iskazivati jake komunikacijske vještine u kombinaciji s rafiniranom diplomacijom. SZP nije (i ne smije biti) "aktivist za privatnost": uz podršku drugih koji upravljaju organizacijom, ta osoba mora igrati ulogu odgovornog omogućavanja redovnog poslovanja i pomoći organizaciji da uključi privatnost u procese donošenja poslovnih odluka, a ne samo otkriti i spriječiti rizike, već također i stvarati vrijednost. Osim toga, GDPR traži da SZP podnosi izvještaje najvišoj razini uprave te da je njegova/njena neovisnost osigurana. Ovo također zahtijeva vještine "čvrstog stajanja na zemlji" i vodstva.

NEOVISNOST

Već smo naveli da "službenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade ili obavljati zadaće na temelju ugovora o djelu" (čl. 37(6)). Međutim, ni u jednom od tih slučajeva to nije radno mjesto običnog zaposlenika ili izvođača. Posebice, Uredba naglašava da:

Takvi službenici za zaštitu podataka, bez obzira jesu li zaposlenici voditelja obrade, trebali bi moći obavljati svoje obveze i zadaće na **neovisan** način. (Uvodna izjava 97) Podrobnije, Uredba propisuje:

> Voditelj obrade i izvršitelj obrade osiguravaju da **službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja tih zadaća**. Voditelj obrade ili izvršitelj obrade **ne smiju ga razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća**. Službenik za zaštitu podataka **izravno odgovara najvišoj rukovodećoj razini** voditelja obrade ili izvršitelja obrade (članak 38(3))

269 Network of Data Protection Officers of the EU Institutions and Bodies - Mreža SZP-ova EU institucija i tijela (Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (bilješka (fusnota) 13, prethodno u tekstu), str. 4.
270 *Idem*, str. 6. Mreža daje preporuke kako bi smanjila ove pritiske u kontekstu diskusije o položaju koji se treba dodijeliti SZP-u u dotičnoj organizaciji, kako se objašnjava pod naslovom "*Radno mjesto SZP-a unutar organizacije*", dalje u tekstu.
271 CEDPO, Choosing the best candidate as your Data Protection Officer (SZP) – Practical guidelines for organisations (Odabir najboljeg kandidata za Vašeg Službenika za zaštitu podataka (SZP) - Praktične smjernice za organizacije) (bilješka (odabir) 8, prethodno u tekstu), str. 3 (neznatno izmijenjeno).

RS29 ovo objašnjava kako slijedi:[272]

> [Gore navedene odredbe] znače […] da, u ispunjavanju svojih zadaća prema članku 39., SZP-ovi ne smiju dobiti upute kako postupati s predmetom, primjerice, koji se rezultat treba postići, kako istražiti pritužbu ili je li potrebno konzultirati nadzorno tijelo. Nadalje, ne smiju im se davati upute da zauzmu određeni stav o pitanju vezanom za pravo o zaštiti podataka, primjerice, posebno u pogledu tumačenja zakona.
>
> Autonomija SZP-a, međutim, ne znači da imaju ovlasti donositi odluke izvan svojih zadaća sukladno članku 39. Voditelj obrade ili izvršitelj obrade ostaju odgovorni za sukladnost sa zakonom o zaštiti podataka i moraju biti u mogućnosti ju dokazati. Ako voditelj obrade ili izvršitelj obrade donesu odluke koje su nespojive s GDPR-om i savjetom SZP-a, SZP-u uvijek treba biti dana mogućnost jasno iznijeti svoje izdvojeno mišljenje o donošenju takvih odluka.

Kako je dalje navedeno u 3. dijelu, savjet SZP-a – i bilo koje radnje poduzete suprotno tom savjetu – trebaju biti zabilježene, a bilo koje ignoriranje savjeta može se iznijeti protiv voditelja ili izvršitelja obrade u bilo kojoj naknadnoj istrazi nadležnog tijela za zaštitu podataka. (Kako je navedeno ranije, suprotno tome, činjenica da su voditelj ili izvršitelj obrade postupali sukladno bilo kojem savjetu ili smjernici njihovog SZP-a može predstavljati "element" za dokazivanje sukladnosti s GDPR-om (Uvodna izjava 77).[273]

RS29 također pojašnjava opseg primjene odredbe koja kaže da SZP-a "voditelj ili izvršitelj obrade ne smiju […] razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća":[274]

> Ovaj zahtjev također ojačava autonomiju SZP-ova i pomaže osigurati da oni djeluju neovisno i uživaju dostatnu zaštitu u izvršavanju svojih zadaća zaštite podataka.
>
> Kazne su zabranjene prema GDPR-u samo ako su nametnute kao rezultat SZP-ovog izvršavanja njegovih zadaća u svojstvu SZP-a. Primjerice, SZP može smatrati da će određena obrada vjerojatno prouzročiti visok rizik pa može savjetovati voditelja ili izvršitelja obrade da provedu procjenu učinka na zaštitu podataka, ali voditelj ili izvršitelj obrade se ne slažu s procjenom SZP-a. U takvoj situaciji, SZP ne može dobiti otkaz za davanje takvog savjeta.
>
> Kazne mogu biti izrečene u mnogo oblika i mogu biti izravne ili neizravne. Mogu se, primjerice, sastojati u neodobravanju ili odugovlačenju napredovanja; sprječavanju napretka karijere; uskraćivanju nekih prednosti koje drugi zaposlenici dobivaju. Nije nužno da su te kazne doista i provedene, dostatna je i sama prijetnja ukoliko se koristi za kažnjavanje SZP-a na temelju nečega vezanog za aktivnosti SZP-a.
>
> Po uobičajenom pravilu vođenja poslovanja, koje bi također bilo primijenjeno i na bilo kojeg drugog zaposlenika ili izvođača, a sukladno pozitivnom nacionalnom građanskom ili radnom ili kaznenom pravu, i SZP-a se može otpustiti zakonito iz drugih razloga osim onih koji se tiču njegovog izvršavanja zadaća u svojstvu SZP-a (primjerice, u slučaju krađe, fizičkog, psihološkog ili seksualnog zlostavljanja ili sličnog ozbiljnog nedoličnog ponašanja).
>
> U ovom kontekstu, treba zamijetiti da GDPR ne specificira kako i kada se SZP-u može uručiti otkaz ili ga zamijeniti drugom osobom. Međutim, što je stabilniji ugovor SZP-a i što više jamstava postoji protiv nepoštenog otkaza, to je vjerojatnije da će on/a biti u mogućnosti postupati neovisno. Stoga, RS29 smatra bilo koje napore organizacije u tom smjeru dobrodošlima.

272 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), odlomak 3.3, str. 14-15.
273 Vidjeti tekst pod točkom 2.2.2, prethodno u tekstu.
274 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu), odlomak 3.4, str. 15.

U najmanju ruku, bilo koji ugovor o radu koji se nudi SZP-u treba uključivati odredbe koje ponavljaju klauzule o neovisnosti iz GDPR-a, ili se treba pozivati na iste. Arbitražni tribunal ili sudovi koji donose odluku o predmetima o otkazu trebaju naravno uzeti odredbe GDPR-a potpuno u obzir. Kada je to potrebno, može biti korisno izmijeniti zakone o radu u tom smislu. Države članice bi također mogle naglasiti neovisnost SZP-ova u drugim nacionalnim zakonima: primjeri zaštitnih mjera od otkaza određenog osoblja mogu se naći u zakonima koji pružaju posebnu zaštitu za, npr. sindikalne dužnosnike, i/ili koji zahtijevaju odobrenje radničkog vijeća za imenovanja i otpuštanja s određenih radnih mjesta.

NB: SZP-ovi zaposleni u EU institucijama raspravljaju pitanja neovisnosti i sukoba interesa (to je sljedeće pitanje obrađeno u ovom Priručniku) uglavnom u smislu ugovornih zaštitnih mjera, dužine imenovanja i ostalih zaštitnih mjera, kako je to opisano kasnije u tekstu, pod naslovom "*Radno mjesto SZP-a unutar organizacije*". CEDPO opaža da organizacija koja imenuje SZP-a treba "razmotriti … kako osigurati neovisnost SZP-a".[275]

SUKOBI INTERESA

Kako RS29 primjećuje:[276]

> Članak 38(6) omogućava SZP-u da 'može ispunjavati i druge zadaće i obveze. Međutim, njime se traži da organizacija osigura 'da takve zadaće i obveze ne dovedu do sukoba interesa'.
>
> Odsustvo sukoba interesa je usko povezano sa zahtjevom neovisnog postupanja. Premda je SZP-ovima dopušteno imati druge funkcije, njima se jedino mogu povjeriti druge zadaće i obveze pod uvjetom da iste ne dovedu do sukoba interesa. Ovo uključuje posebice to da SZP ne može biti na položaju unutar organizacije koji ga vodi tome da odredi svrhe i sredstva obrade osobnih podataka. Zbog specifične organizacijske strukture u svakoj organizaciji, ovo treba biti razmotreno za svaki pojedini slučaj zasebno.
>
> Kao opće pravilo, konfliktne pozicije mogu uključivati pozicije više uprave (kao što su glavni izvršni direktor, glavni direktor operacija, glavni financijski direktor, glavni medicinski službenik, voditelj odjela marketinga, voditelj Odjela za ljudske resurse ili voditelj IT odjela), ali također i druge uloge niže pozicionirane u organizacijskoj strukturi, ako takve pozicije ili uloge vode do utvrđivanja svrha ili sredstava obrade.
>
> Ovisno o djelatnostima, veličini i strukturi organizacije, mogla bi biti dobra praksa za voditelje obrade ili izvršitelje obrade:
>
> - identificirati pozicije (radna mjesta) koje bi bile nespojive s funkcijom SZP-a
> - sastaviti interna pravila u tom smislu kako bi se izbjegli sukobi interesa
> - uključiti općenitije objašnjenje o sukobima interesa
> - objaviti da njihov SZP nije u sukobu interesa u pogledu svoje funkcije kao SZP, kao način podizanja svijesti o ovom zahtjevu iz Uredbe
> - uključiti zaštitne mjere u interna pravila organizacije i osigurati da su obavijest o slobodnom radnom mjestu za poziciju SZP-a ili ugovor o djelu dovoljno precizni i detaljni kako bi se izbjegao sukob interesa. U tom kontekstu, treba isto imati na umu da sukobi interesa mogu poprimati različite oblike, ovisno o tome je li SZP došao na to radno mjesto iz same organizacije ili iz neke druge.

275 CEDPO, Choosing the best candidate as your Data Protection Officer (SZP) – Practical guidelines for organisations (Odabir najboljeg kandidata…) (bilješka (fusnota) 8, prethodno u tekstu), str. 3.
276 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 11, prethodno u tekstu, odlomak 3.5, str. 15-16. Treći stavak ("Kao opće pravilo …") javlja se kao bilješka (fusnota) u dokumentu, a ne u glavnom tekstu, kao što je ovdje slučaj.

SZP-i zaposleni u EU institucijama dodaju:[277]

> SZP ne smije biti u sukobu interesa između dužnosti SZP-a i bilo kojih drugih službenih dužnosti, posebice u odnosu na primjenu odredbi Uredbe (čl. 24.3). Sukob interesa prisutan je kada ostale dužnosti, koje se traži da SZP obavlja, mogu imati izravno suprotne interese onima zaštite osobnih podataka unutar njegove/njene institucije. Ako je potrebno, SZP treba pokrenuti ovo pitanje s tijelom koje ga/ju je imenovalo.

Oni se bave ovim pitanjem detaljnije u smislu ugovornih zaštitnih mjera, dužine imenovanja i drugih zaštitnih mjera, kako je opisano pod sljedećim naslovom. CEDPO ponovo samo primjećuje da, ako SZP-ovo imenovanje nije na puno radno vrijeme, organizacija koja ga/ju je imenovala treba "razmotriti … kako riješiti sukob interesa".[278]

RADNO MJESTO SZP-A UNUTAR ORGANIZACIJE

Hijerarhijska i ugovorna pozicija SZP-a unutar organizacije je ključna u odnosu na osiguravanje SZP-ove učinkovitosti, neovisnosti i izbjegavanja sukoba interesa.

S druge strane, kako je navedeno ranije u tekstu, SZP bi trebao biti "blizak" organizaciji u kojoj obavlja svoj posao (vidjeti u tekstu ranije, pod naslovom "*Tražena stručnost*"). Štoviše, kako je to CEDPO formulirao:[279]

> Da bi SZP bio učinkovit, [on ili ona] treba biti dostupan "na terenu", a ne samo dostupan različitim dionicima unutar organizacije, već proaktivno tražiti mogućnosti interakcije s različitim odjelima.

Ovo može biti problematično u slučajevima kada vanjski SZP-ovi rade na ugovor o djelu: oni po definiciji nisu dio tijela kojem pomažu. U privatnom sektoru, zasigurno mogu postojati – a u nekim državama, poput Njemačke, nedvojbeno i postoje – vanjski SZP-ovi s opsežnom stručnošću u privatnom sektoru ili podsektoru u kojem rade. U javnom sektoru, to može biti teže – (usp. 2.3.2, ranije u tekstu, pod naslovima "*SZP-ovi za javna tijela većeg kapaciteta ili grupe tijela*" i "*Vanjski SZP-ovi*").

Ali uvijek postoji tenzija između, s jedne strane, nužne "blizine" SZP-a njegovoj/njenoj organizaciji, te, s druge strane, potrebe izbjegavanja sukoba interesa i osiguravanja stvarne neovisnosti SZP-a u praksi.

Kao što je već ranije spomenuto, u mišljenju RS29, to znači da SZP ne može biti uključen u određivanje svrha i sredstava za obradu osobnih podataka te ne može biti na višem menadžerskom položaju, kao što je glavni izvršni direktor ili glavni direktor, odnosno voditelj glavnog odjela.[280]

Ovim pitanjem se puno detaljnije bave SZP-ovi zaposleni u EU institucijama. Premda se njihova gledišta moraju naravno razmatrati u svjetlu njihovog specifičnog konteksta, ipak je korisno pogledati ih. S obzirom

---

277 Network of Data Protection Officers of the EU Institutions and Bodies (Mreža SZP-a…), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (bilješka (fusnota) 13, prethodno u tekstu), str. 15.

278 CEDPO, Choosing the best candidate as your Data Protection Officer (SZP) – Practical guidelines for organisations (Odabir najboljeg kandidata…) (bilješka (fusnota) 8, prethodno u tekstu), str. 3.

279 Idem, str. 2.

280 Vidjeti ranije, pod naslovom "*Sukobi interesa*", posebice treći stavak u citatu iz Smjernice RS29 o SZP-ovima. Nasuprot tome, **talijansko** tijelo za zaštitu podataka, *Garante*, u svojim FAQs on DPOs (Često postavljana pitanja o SZP-ovima), navodi da:

> … Članak 38(3) propisuje da SZP 'izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade'. Ovaj zahtjev izravnog izvještavanja može osigurati, posebice, da vodeći menadžment bude obaviješten o smjernicama i preporukama koje daje SZP-o, nastupajući u svojoj savjetodavnoj ulozi, odnosno ulozi podizanja svijesti u odnosu na voditelja ili izvršitelja obrade.
>
> Shodno tome, ako se imenuje interni SZP, bilo bi preporučljivo, u načelu, da se imenuju voditelj odjela ili viši član osoblja kad god je to moguće na temelju organizacijske strukture i uzimajući u obzir složenost postupaka obrade.. Na taj način, imenovani SZP će biti u poziciji autonomno i neovisno obavljati svoje zadaće, kao i održavajući vezu izravno s najvišom rukovodećom razinom. (*Garante*, FAQs on DPOs [bilješka (fusnota) 249, ranije u tekstu], odlomak 2.)

Možda najbolji način da se pomire gledišta RS29 i talijanskog *Garante* po ovom pitanju, bilo bi predložiti da se SZP-ovi trebaju imenovati *na razini* voditelja odjela ili višeg menadžmenta, ali bez stvarne odgovornosti za postupke obrade osobnih podataka. [285] Vidi (bilješku) 207, ranije u tekstu.

[286] Network of Data Protection Officers of the EU Institutions and Bodies (Mreža SZP-ova u EU institucijama…), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Profesionalni standardi…) (bilješka (fusnota) 13, ranije u tekstu), str. 6-7.

da su pronašli različite odredbe u uredbi koja regulira njihov posao (Uredba (EZ) 45/2001)[281] što je zamišljeno kako bi jamčilo njihovu neovisnost, oni navode kako slijedi:[282]

U praksi, međutim, SZP-u može biti izazovno da svoje dužnosti obavlja potpuno neovisno. Samo je po sebi razumljivo, individualna situacija i osobnost SZP-a igrat će ulogu, ali se može općenito pretpostaviti da određeni elementi imaju tendenciju oslabjeti poziciju SZP-a:

- SZP zaposlen na nepuno radno vrijeme suočen je sa sukobom između raspoređivanja vremena i napora ispunjavanja svojih zadaća kao SZP nasuprot ostalih zadaća. U pogledu razvoja karijere i ocjene njegove/njene uspješnosti, uprava može staviti veći naglasak na aktivnosti koje ne spadaju u zadaće SZP-a. Ovo stvara pritisak na SZP prilikom fokusiranja svojih napora na obavljanje zadaća u svojstvu SZP-a. SZP zaposlen na nepuno radno vrijeme također je u opasnosti od uplitanja u sukob interesa.
- SZP koji ima ugovor na određeno vrijeme bi vjerojatnije bio u nepovoljnijem položaju ako energično obavlja svoje dužnosti SZP-a negoli SZP s ugovorom o radu na neodređeno (službeni ili privremeni zastupnik s ugovorom na neodređeno vrijeme). Razlog tome je što on/a može biti zabrinut oko toga kako će njegove/njene radnje negativno utjecati na produženje ugovora o radu. SZP koji je vrlo mlad i ima tek ograničeno radno iskustvo, može se susresti s poteškoćama kada se treba suprotstaviti voditelju obrade, te može biti više fokusiran/a na razvoj vlastite karijere negoli na angažirano obavljanje SZP zadaća.
- SZP koji podnosi izvješća izravno nadređenome u hijerarhiji, i kojeg taj nadređeni nadzire (direktor ili voditelj odjela), može osjećati pritisak kod suradnje i neometanog rada s upravom i ostalim kolegama, jer angažirano obavljanje dužnosti SZP-a može imati negativan utjecaj na karijeru… Kako bi se olakšao ovaj pritisak, SZP bi trebao podnositi izvještaje, i biti pod nadzorom administrativnog voditelja institucije ili tijela. Ovo je posebice važno za SZP-ove koji rade na nepuno radno vrijeme, koji trebaju izvještavati i biti pod nadzorom tijela koje ga je imenovalo za zadatke SZP-a, a za druge dužnosti ih uobičajeno nadzire nadređeni u hijerarhiji.
- SZP koji mora zatražiti osoblje i resurse (IT resursi, proračun za poslovna putovanja i edukacije) od svojeg izravno nadređenog, mogao bi se suočiti s poteškoćama ako potonji nije u potpunosti posvećen postizanju sukladnosti zaštite podataka. Ovo se može izbjeći ako SZP ima svoju vlastitu proračunsku odgovornost te ako bilo koji zahtjevi za dodatnim resursima podliježu odobrenju tijela koje ga je imenovalo.

Najbolje prakse koje pomažu osiguravanju neovisnosti SZP-a jesu:

- Institucija ili tijelo treba ustanoviti radno mjesto SZP-a unutar organizacije kao mjesto Savjetnika, Voditelja odjela ili Direktora, a u svakom slučaju radno mjesto treba biti službeno priznato kao razina uprave, na službenoj organizacijskoj shemi (sistematizaciji) institucije/tijela;
- Institucija ili tijelo trebaju imenovati SZP na najduže moguće vrijeme, u svjetlu SZP-ovog ugovora. Stoga bi petogodišnje imenovanje trebalo biti norma, osim ako to nije moguće u danim okolnostima;
- SZP treba imati trajni ugovor/na neodređeno s institucijom ili tijelom [i] treba imati dovoljno iskustva (…);
- SZP treba moći posvetiti svoje vrijeme u cijelosti svojim zadaćama SZP-a, posebno u slučaju velikih institucija i tijela, a kod manjih tijela - u inicijalnoj fazi uspostavljanja režima zaštite podataka. Pravilna podrška u smislu resursa i infrastrukture treba biti osigurana. Zadaće koje nisu u djelokrugu SZP-a u slučaju SZP-a koji radi na nepuno radno vrijeme ne smiju dovoditi do sukoba interesa, čak ni do sumnje na sukob interesa sa zadaćama SZP-a;

281 Vidi (fusnotu) 207, ranije u tekstu.
282 Network of Data Protection Officers of the EU Institutions and Bodies (Mreža DPO-ova u EU institucijama…), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (Profesionalni standardi…) (bilješka (fusnota) 13, ranje u tekstu), str. 6 – 7.

- SZP-ovi u organizacijama gdje je obrada podataka osnovna djelatnost organizacije uobičajeno će trebati različite članove osoblja. Takav kapacitet osoblja treba biti osiguran;
- Trebaju postojati pravila unutar organizacije koja osiguravaju obvezu svih članova osoblja da surađuju s SZP-om, bez da je potrebno čekati naredbu ili dopuštenje njihovog nadređenog;
- SZP treba podnositi izvještaje voditelju institucije ili tijela, koji bi trebao biti odgovoran za praćenje kako SZP provodi svoje zadaće, kao što je utvrđeno Uredbom. Osoba odgovorna za praćenje rada SZP-a treba biti osjetljiva na potrebu SZP-a da zauzme snažno stav, što ostali unutar organizacije možda neće cijeniti. SZP ne smije trpjeti bilo kakve predrasude na ime obavljanja svojih zadaća. Tijelo koje ga je imenovalo treba osigurati da tijekom mandata SZP-a, on/ona ostvare barem "uobičajeno" profesionalno napredovanje u karijeri. Kod ocjenjivanja radnog učinka SZP-a, ocjenjivač treba biti oprezan kako ne bi ukorio SZP zbog zauzimanja nepopularnih pozicija niti treba razmatrati zahtjeve za zaštitu podataka kao administrativni teret. Za SZP koji radi u nepunom radnom vremenu, ispunjavanje zadaća SZP-a treba biti jednake težine u usporedbi s ispunjavanjem zadaća koje nisu u djelokrugu SZP-a… ;
- SZP treba imati svoju vlastitu proračunsku liniju, postavljenu sukladno relevantnim pravilima i procedurama dotične institucije/tijela; zahtjevi SZP-a za bilo kojim daljnjim resursima trebaju podlijegati odobrenju administrativnog voditelja. Drugi su aranžmani prihvatljivi ako osiguravaju SZP-u resurse koji su mu/joj potrebni za ispunjenje njegove/njene misije na neovisan način;
- SZP treba imati ovlasti za potpisivanje korespondencije koja se tiče zaštite podataka.

TZP-i mogu smatrati prikladnim izdati detaljne smjernice u vezi s tim, sukladno gore navedenom.

RESURSI I PROSTORIJE

GDPR propisuje kako slijedi:

> Voditelj obrade i izvršitelj obrade podupiru službenika za zaštitu podataka u izvršavanju zadaća iz članka 39. [kako je opisano pod točkom 2.3.4, dalje u tekstu, pod tim naslovom] **pružajući mu potrebna sredstva za izvršavanje tih zadaća** i ostvarivanje pristupa osobnim podacima i postupcima obrade te za održavanje njegova stručnog znanja (članak 38(2)).

Na tu temu, RS29 posebice predlaže sljedeće:[283]

- Aktivnu podršku funkciji SZP-u od strane viših upravljačkih struktura (primjerice kao na razini uprave).
- Dostatno vrijeme da bi SZP-ovi mogli ispuniti svoje zadaće. Ovo je posebice važno kada je SZP imenovan u nepunom radnom vremenu ili ako zaposlenik obavlja poslove zaštite podataka pored ostalih zadaća. U suprotnom, sukobljeni prioriteti bi mogli dovesti do zanemarivanja zadaća SZP-a. Dovoljno vremena kojeg SZP treba posvetiti svojim zadaćama SZP-a je od presudne važnosti. Dobra je praksa ustanoviti postotak vremena za funkciju SZP-a kada se te zadaće ne obavljaju u punom radnom vremenu. Također je dobra praksa odrediti vrijeme potrebno za obavljanje funkcije, odgovarajuće razine prioriteta za obveze SZP-a te da SZP (ili organizacija) sastavi radni plan za obveza SZP-a.
- Primjerena podrška u smislu financijskih resursa, infrastrukture (prostor, sadržaji, oprema) i osoblje, kada je to prikladno.
- Službeni dopis o imenovanju SZP-a upućen svom osoblju kako bi se osiguralo da postojanje i funkcija SZP-a budu poznate unutar organizacije.

283 Smjernice RS29 o SZP-ovima (bilješka (fusnota) 242, prethodno u tekstu), odlomak 3.2, str. 13-14.

- Potreban pristup drugim odjelima, primjerice Ljudskim resursima, Pravnom odjelu, IT-u, Osiguranju itd., tako da SZP-ovi mogu primiti bitnu podršku, dobiti input i informacije od tih drugih odjela.
- Trajna edukacija. [Vidjeti ranije navedeno, pod naslovom "*Formalna edukacija i Certifikacije*"]
- S obzirom na veličinu i strukturu organizacije, moguće je potrebno osnovati SZP tim (SZP i njegovo/njeno osoblje). U takvim slučajevima, interna struktura tima i zadaće, te odgovornosti svakog člana trebale bi biti jasno opisane. Slično tome, kada funkciju SZP-a obavlja vanjski pružatelj usluga, tim pojedinaca koji radi za tu osobu može učinkovito obavljati zadaće SZP-a kao tim, uz odgovornost imenovane glavne kontakt osobe za klijenta.

Općenito, što su postupci obrade složeniji i/ili osjetljiviji, to se više resursa mora dodijeliti SZP-u. Funkcija zaštite podataka mora biti učinkovita i dostatno financirana u odnosu na zaštitu podataka koja se obavlja.

Kako je već navedeno, SZP-ovi zaposleni u EU institucijama smatraju da "SZP koji mora zatražiti osoblje i resurse (IT resursi, proračun za poslovna putovanja i edukacije) od svojeg izravno nadređenog, može se suočiti s poteškoćama ako potonji nije u potpunosti posvećen postizanju sukladnosti zaštite podataka". Oni stoga preporučuju da se SZP-u dodijeli vlastita proračunska odgovornost, pri čemu bilo koji zahtjevi za dodatnim resursima koji su postavljeni budu podložni odobrenju tijela koje je imenovalo SZP-a (a ne izravno nadređenom).[284] CEDPO navodi:

> Kod složenih organizacija, trebat ćete razmisliti hoće li SZP-u pomagati ili ne druge osobe interno, koje će nadopunjavati njegove/njene sposobnosti/vještine, na trajnoj osnovi (SZP tim) ili prema potrebi s vremena na vrijeme (vanjski savjetnik?).

U javnim tijelima – doista se preporučuje osnivanje tima. U malim javnim tijelima, tim bi se mogao sastojati samo od postojećeg osoblja koje se redovito sastaje s SZP-om da raspravi relevantna pitanja i pripremi pravila (politiku). U većim tijelima, neki mogu formalno biti imenovani za pomoćne funkcije SZP-u na nepuno radno vrijeme. Kod nekih, može biti potrebno imenovati osoblje na puno radno vrijeme za podršku SZP-u. Kako svi dokumenti koji sadrže smjernice jasno naglašavaju, odluka o tim pitanjima treba se donijeti u svjetlu (i) složenosti ili osjetljivosti postupaka obrade osobnih podataka, i (ii) veličine i resursa dotičnog tijela. Ali, na kraju, zakonski je zahtjev GDPR-a da resursi dodijeljeni SZP-u (i timu) budu primjereni za postojeće zadaće.

OVLASTI SZP-A

Osim resursa, te dostatno snažne, zaštićene i više pozicionirane pozicije unutar organizacije, SZP također treba imati ovlast obavljati svoje zadaće. Članak 38(2) (citiran pod prethodnim naslovom) jasno navodi da radi toga tijelo koje imenuje SZP mora osigurati da on ili ona imaju "pristup" osobnim podacima i postupcima obrade. Ovo treba shvatiti na isti način kao i odgovarajuću odredbu u uredbi koja obuhvaća SZP-ove zaposlene u EU institucijama, čl. 24(6) Uredbe (EZ) 45/2001, a SZP-ovi je ovako tumače:[285]

> Uredba zahtijeva od voditelja obrade da pomognu SZP-u u obavljanju njegovih/njenih zadaća i da pružaju odgovore na postavljena pitanja te navodi da SZP mora u svako doba imati pristup podacima koji su predmet postupaka obrade i svim uredima, instalacijama za obradu podataka te nosačima podataka.
>
> Premda SZP nema ovlasti provedbe u odnosu na izvršitelje, on/a ima ovlast nadzirati sukladnost prikupljanjem svih odgovarajućih podataka, koje su tijelo koje je imenovalo SZP i njegovi izvršitelji obrade dužni učiniti dostupnima.

284 Vidjeti prethodno u tekstu, pod naslovom "*Radno mjesto SZP-a unutar organizacije*".
285 Network of Data Protection Officers of the EU Institutions and Bodies (Mreža SZP-ova u EU institucijama…), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (bilješka (fusnota) 244, prethodno u tekstu), str. 12. Bitno je primijetiti, za razliku od čl. 38(2) GDPR-a, čl. 24(6) Uredbe (EZ) 45/2001 zapravo ne spominje izrijekom pristup osobnim podacima i postupke obrade osobnih podataka. To se stoga, u potonjem kontekstu, tumači kao općenitija odredba o pružanju nužnih resursa. Na to je vjerojatno utjecala specifičnija, jača odredba o pristupu takvim informacijama koji se mora osigurati ENZP-u (unutar EU institucija).

Ostali komentari SZP-ova zaposlenih u EU institucijama u odnosu na obveze SZP-a za osiguranjem sukladnosti s pravilima o zaštiti podataka također su relevantni:[286]

> IT alati mogu se razviti kako bi pomogli SZP-u u obavljanju redovitog nadzora. Administrativni aranžmani se također mogu odrediti, kao primjerice oni koji osiguravaju da SZP dobiva kopiju sve pošte u kojoj se postavljaju pitanja o zaštiti podataka te koji traže savjetovanje s SZP-om o dokumentima u kojima se postavljaju pitanja o zaštiti podataka. Pazite, redovito praćenje sukladnosti i izvještavanje o rezultatima može stvoriti veliki pritisak na izvršitelje kako bi osigurali da su njihovi postupci obrade sukladni. Redovito praćenje i izvještavanje su stoga najjači alati za osiguravanje sukladnosti. U tom cilju, predavanje godišnjeg izvješća upravi … je najbolja praksa.

Posebna se pitanja javljaju kada voditelj ili izvršitelj odbiju poslušati savjet svog SZP-a. Riječima radne skupine RS29:[287]

Ako voditelj ili izvršitelj obrade donese odluke koje su nekompatibilne s GDPR-om i savjetom SZP-a, SZP treba imati mogućnost jasno izraziti svoje izdvojeno mišljenje najvišoj razini uprave i onima koji donose odluke. U tom pogledu, članak 38(3) propisuje da SZP 'izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade'. Takvo izravno izvješćivanje osigurava da viši menadžment (npr. uprava) budu svjesni savjeta i preporuka SZP-a kao dijela SZP-ove misije informiranja i savjetovanja voditelja obrade i izvršitelja. Još jedan primjer izravnog izvješćivanja je sastavljanje godišnjeg izvještaja o aktivnostima SZP-a koje se predaje najvišoj rukovodećoj razini.

Premda ne postoji posebna obveza propisana u GDPR-u da SZP izvijesti državne vlasti o nesukladnosti sa zakonom, GDPR ipak propisuje da je jedna od zadaća SZP-a:

> djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i […] **savjetovanje, prema potrebi**, o svim drugim pitanjima (čl. 39(1)(e), dodatno naglašeno)

U slučajevima kada SZP smatra da njegov/njen poslodavac djeluje kršeći zakon, SZP stoga zasigurno ima ovlast – i zapravo, mi bismo čak rekli, obvezu – postaviti to pitanje nacionalnom TZP-u, da bi se problem riješio. Ovime se ilustrira delikatnost SZP-ovog položaja.

U isto vrijeme, kako RS29 ispravno naglašava:[288]

> Autonomija SZP-ova, međutim, ne znači da oni imaju ovlasti donositi odluke koje imaju doseg izvan njihovih zadaća sukladno članku 39.
>
> Voditelj ili izvršitelj obrade ostaju odgovorni za sukladnost s pravom o zaštiti podataka i moraju biti u mogućnosti dokazati sukladnost.

FORMALNOSTI

Svi gore navedeni zahtjevi itd. u odnosu na SZP trebaju se jasno oslikavati u pravnom dokumentu po kojem je SZP imenovan. Kako navodi talijansko tijelo za zaštitu podataka, *Garante del Privacy*, u svojim FAQs on DPOs (Često postavljana pitanja o SZP-u):[289]

286 *Idem.*

287 Smjernice RS29 o SZP-ovima (bilješka (fusnota 242, prethodno u tekstu), str. 15. Isti je pristup zauzet i od strane Mreže SZP-ova zaposlenih u EU institucijama, vidjeti ponovo Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (bilješka (fusnota) 246, prethodno u tekstu), str. 12 (vidjeti stavak nakon onoga citiranog, prethodno u tekstu).

288 Smjernice RS29 o SZP-ovima, str. 15, s pozivom na načelo "pouzdanosti" [**odgovornosti**] iz čl. 5(2) GDPR-a.

289 *Garante*, FAQs on DPOs (Često postavljana pitanja o SZP-ovima) (bilješka (fusnota) 249, prethodno u tekstu), odlomak 1. *Garante* je priložio **model obrazac za imenovanje [imenovanje SZP-a]** uz često postavljana pitanja (FAQs) radi lakšeg snalaženja **Model form for communicating the DPO's data to the Garante** (Model obrasca za priopćavanje podataka o SZP-u tijelu Garante) te ga također ovdje prilažem.

Članak 37(1) GDPR-a predviđa da voditelj obrade i izvršitelj obrade imenuju SZP. Shodno tome, postojanje instrumenta (dokumenta) kojim se imenuje SZP je sastavni dio bilo kojeg aranžmana za ispunjenje relevantnih obveza.

Ako je kandidat za SZP član osoblja, mora se izraditi *ad hoc* instrument kojim ga se imenuje kao SZP. Nasuprot toga, ako se odabire vanjska osoba, formalno imenovanje te osobe kao SZP-a bit će integralni dio *ad hoc* ugovora o pružanju usluga koji treba sročiti sukladno članku 37 GDPR-a (…).

Neovisno o prirodi i vrsti pravnog instrumenta, potonje mora navoditi nedvosmisleno tko će biti SZP, navođenjem imena osobe, dodijeljenih zadaća (koje mogu i premašivati

zadaće predviđene člankom 39. GDPR-a) i obveze koje se odnose na podršku za koju se očekuje da će SZP pružiti voditelju obrade/izvršitelju obrade sukladno važećem zakonskom i regulatornom okviru.

Ako su SZP-u dodijeljene dodatne zadaće, povrh ovih navedenih početno u dokumentu o imenovanju, taj ugovor ili ugovor o pružanju usluga će se morati izmijeniti i/ili dopuniti na odgovarajući način.

Dokument o imenovanju i/ili ugovor o pružanju usluga trebaju također navoditi, na koncizan način, razloge zašto je dotična fizička osoba imenovana kao SZP od strane javnog tijela ili tijela s javnim ovlastima, tako da se može utvrditi sukladnost sa zahtjevima sukladno članku 37(5) GDPR-a; u tom cilju, može se pozvati na ishod interne ili vanjske procedure odabira kandidata. Specifikacija kriterija primijenjenih prije imenovanja određenog kandidata nije samo znak transparentnosti i dobrog upravljanja, već također i element kojeg se treba uračunati kod ocjenjivanja sukladnosti s načelom "pouzdanosti".

Po imenovanju SZP-a, voditelj obrade ili izvršitelj obrade moraju uključiti kontaktne podatke SZP-a u informacije koje se daju ispitanicima i objaviti te podatke na relevantnim mrežnim stranicama; također se traži priopćavanje podataka tijelu za zaštitu podataka Garante, sukladno članku 37(7). Što se tiče objave na mrežnim stranicama, može biti prikladno objaviti kontaktne podatke SZP-a u odjeljku mrežnih stranica o

"transparentnosti" ili "otvorenosti", kao i na stranici o "pravilima privatnosti" – gdje je to moguće.

Kako se pojašnjava u Smjernicama [RS29], ime SZP-a ne mora biti objavljeno sukladno članku 37(7); međutim, to bi mogla biti dobra praksa u javnom sektoru. Za razliku od toga, kontaktni podaci moraju se dostaviti tijelu za zaštitu podataka Garante kako bi se olakšala međusobna interakcija (…) S druge strane, kontaktni podaci SZP-a moraju se priopćiti ispitanicima u slučaju povrede osobnih podataka (vidjeti članak 33(3)b).

2.5.4 Funkcije i zadaće SZP-a (Pregled)

U odnosu na SZP-ove zaposlene u EU institucijama, ENZP razlikuje sljedećih **sedam funkcija SZP-a**:[290]

- Funkcija povećanja informiranosti i podizanja svijesti [o pitanjima zaštite podataka];
- Savjetodavna funkcija;
- Organizacijska funkcija;
- Funkcija suradnje;
- Funkcija praćenja sukladnosti;
- Funkcija rješavanja upita ili prigovora; i
- Funkcija provedbe.

290 EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (bilješka (fusnota) 243, prethodno u tekstu), str. 6-7.

SZP-ovi imenovani po osnovi GDPR-a obavljaju uglavnom slične funkcije. One koreliraju rasponu određenijih **zadaća**, navedenih uz korištenje širokih pojmova u članku 39. GDPR-a:

Članak 39.

Zadaće službenika za zaštitu podataka

1. Službenik za zaštitu podataka obavlja najmanje sljedeće zadaće:
   (a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka;
   (b) praćenje poštivanja ove Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;
   (c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35;
   (d) suradnja s nadzornim tijelom;
   (e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36 te savjetovanje, prema potrebi, o svim drugim pitanjima.
2. Službenik za zaštitu podataka pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade.

U praksi, SZP će se, naravno, uključiti i u određene zadatke koji su službeno dodijeljeni voditelju, u tome što će većina voditelja (osim ako oni sami nemaju relevantnu, dubinsku stručnost izvan ureda svojeg SZP-a, npr. u njihovom pravnom odjelu ili odjelu za usklađenost) tražiti pomoć od svojeg SZP-a u obavljanju tih zadataka. Zapravo, to je blago rečeno: u mnogim slučajevima, voditelji kada se suoče s njihovim novim, zahtjevnim odgovornostima u okviru GDPR-a (posebno pod novom odgovornošću/dokazivanjem ispunjavanja obveza) će gledati da SZP učini veći dio posla, čak i ako, kao što je to izričito izneseno u GDPR-u u raznim aspektima, u zakonu ostaje voditelj taj, a ne SZP, koji je odgovoran i dužan odgovarati za bilo kakve propuste u tom pogledu.

Kako je jasno sadržano u članku 5(2) GDPR-a:

Voditelj obrade odgovoran je za usklađenost […][s različitim zahtjevima iz GDPR-a] *te je mora biti u mogućnosti dokazati,*

Drugim riječima, ta odgovornost ne pada na SZP – što je također jasno iz članka 39, citiranog ranije u tekstu, koji naglašava savjetodavne zadaće SZP-a i zadaće pružanja podrške.

Međutim, SZP je i dalje ključan u tom smislu, da mora, putem svojeg savjeta, višim razinama rukovodećeg osoblja i niže pozicioniranom osoblju omogućiti da udovolje relevantnim obvezama. Suprotno tome, najviša razina uprave kao i niža dužne su savjetovati se s SZP-om ako se pojave pitanja sukladnosti s GDPR-om.

ENZP je izradio korisnu, tzv. RACI ("**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed" – "Nadležan, Odgovoran, Savjetovan, Informiran") matricu u tom smislu, koja je primjenjiva naročito u odnosu na vođenje evidencije o postupcima obrade osobnih podataka:[291]

291 EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (Odgovornost temeljem I. dijela: Evidencije, registri i kada provesti Procjenu učinka na zaštitu podataka), veljača 2018, str. 4, dostupno na: https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf Moglo bi se dodati lijevom stupcu, "Ispitanici" i "Tijelo za zaštitu podataka", s "X-ovima" za njih u posljednjem stupcu ("Informiran"), ali relevantne zadaće su u biti složenije negoli što bi se moglo na ovaj način označiti: ispitanici trebaju biti obaviješteni o određenim pitanjima u mnogim slučajevima (ili od strane voditelja obrade na njegovu inicijativu ili na zahtjev), ali ne uvijek o svemu, a SZP mora u nekim slučajevima biti ne samo informiran, već se

	Responsible (nadležan)	Accountable (odgovoran)	Consulted (savjetovan)	Informed (informiran)
Vodeći menadžment		X		
"Vlasnik posla"	X			
SZP			X	
IT odjel			X	
Izvršitelji, ako postoje			X	

Dodao je sljedeće pojašnjenje terminologije:[292]

> "**Responsible"** (nadležan) znači osobu koja ima obvezu djelovati i donositi odluke da bi se postigli traženi ishodi (zadaci); "**Accountable"** (odgovoran) znači odgovarati za svoje radnje, odluke i postignute rezultate; "**Consulted"** (savjetovan) znači da se osobu pitalo da doprinese i pruži savjete/komentare; "**informed"** (informiran) znači da je osoba stalno obaviještena o odlukama koje su donesene i o procesu.

ENZP koristi termin "**vlasnik posla**" za osobu koja je odgovorna, u praktičnom smislu, za relevantni postupak obrade: "vlasnik" procesa. Kako se dalje objašnjava u nastavku, pod naslovom "*Preliminarna zadaća*", to će biti dio prvih zadaća SZP-a, izraditi ovu internu raspodjelu odgovornosti.

Sukladno navedenom, u pregledu SZP-ovih zadaća, u nastavku, ove će zadaće često biti opisivane kao "pomaganje voditelju obrade osigurati" za različita pitanja, ili pak kao

"savjetovanje voditelja obrade" (ili dotičnog "vlasnika posla"/člana osoblja) o tome kako postići određene ciljeve, a ne "osiguravati" ta pitanja ili diktirati kako se tim pitanjima treba pristupiti. U praksi, posebno u malim organizacijama, moguće je da će SZP sam ponijeti veći dio nekih od tih tereta, ali formalno to i dalje ostaje odgovornost voditelja obrade (i interno, dotičnog odgovornog "vlasnika posla"/ člana osoblja).

Iz navedenog, i uzimajući *u obzir* ovo upozorenje o neodgovornosti SZP-a, zaključujemo petnaest zadataka SZP-a, ili koji će u praksi uključivati SZP (plus Pripremni zadatak), koji se može grupirati pod sedam naslova funkcija koje je utvrdio Europski nadzornik za zaštitu podataka, kako je navedeno na početku završnog dijela ovog priručnika, Treći dio.

Dovoljno je napomenuti da su te funkcije i zadaci, s druge strane, jasno i čvrsto povezani s "načelom pouzdanosti" i povezanom "demonstracijom obveza usklađenosti" nametnuti voditelju obrade, o čemu smo ranije raspravljali, u odjeljku 2.4 ovog priručnika.

U sljedećem dijelu ovog priručnika (treći dio) pružamo smjernice o tome kako voditelj obrade i SZP trebaju izvršavati te zadatke. Prvo, međutim, važno je ponoviti da - iako će SZP imati značajan utjecaj i doprinos u odnosu na gore navedene zadatke, on nema nikakvu osobnu formalnu odgovornost za poštivanje GDPR-a.

Naravno, SZP će morati uspostaviti strategiju kako bi mogao izvršiti sve zadatke, u skladu s programom po godini ili semestru s određenom fleksibilnošću u pogledu mogućih neočekivanih problema (kao što je nagli problem zaštite podataka ili povreda osobnih podataka koja utječe na organizaciju, ili gdje TZP odlučuje istražiti njegovu organizaciju).

mora provesti i savjetovanje s SZP-om. U svakom slučaju, matrica cilja na razjašnjavanje pitanja unutar organizacije voditelja obrade, a ne u odnosu na vanjska tijela.[296] *Idem*, bilješka (fusnota) 7 (dodan naglasak u fontu **podebljano**).

292 Idem, bilješka (fusnota) 7

TREĆI DIO

Praktične smjernice o zadaćama SZP-a ili zadaćama koje će u praksi uključivati SZP-a

("ZADAĆE SZP-A")

Ovaj dio priručnika namijenjen je pružanju praktičnih smjernica o **zadaćama SZP-a, ili zadaćama koje će u praksi uključivati SZP,** koje su već navedene pod točkom 2.5.4, ranije u tekstu, te su ponovo iznesene u nastavku. Kratkoće radi, s vremena na vrijeme ćemo se na njih pozivati terminom "Zadaće SZP-a". Kako je navedeno u tom odlomku, petnaest zadaća izvedeno je iz popisa zadaća koje su široko navedene u članku 39. GDPR-a, grupirane pod **sedam funkcija SZP-a,** koje je identificirao ENZP. U raznim odlomcima u kojima se raspravlja o zadaćama, nudimo **primjere** koji ih ilustriraju, vezano za stvarnu praksu.

Zadaće SZP-a:

Preliminarna zadaća:

Istraživanje okoline voditelja obrade

Organizacijske funkcije:

Zadaća 1: Stvaranje evidencija aktivnosti obrade osobnih podataka

Zadaća 2: Preispitivanje postupaka obrade osobnih podatka

Zadaća 3: Procjenjivanje rizika nametnutih postupcima obrade osobnih podataka

Zadaća 4: Rješavanje postupaka obrade koji će potencijalno rezultirati/dovesti do "visokog rizika": provođenje procjene učinka na zaštitu podataka (PUZP)

Funkcije praćenja poštivanja uredbe:

Zadaća 5: Kontinuirano ponavljanje zadaća 1 – 3 (i 4)

Zadaća 6: Rješavanje povreda osobnih podataka

Zadaća 7: Istražna zadaća (uključujući rješavanje internih pritužbi)

Savjetodavne funkcije:

Zadaća 8: Savjetodavna zadaća – općenito

Zadaća 9: Podržavanje i promoviranje "Tehničke i integrirane zaštite podataka"

Zadaća 10: Savjetovanje o i praćenje sukladnosti s politikama (pravilima) zaštite podatka, ugovori između zajedničkih voditelja obrade, voditelja obrade -voditelja obrade i voditelja obrade - izvršitelja obrade, Obvezujuća korporativna pravila i klauzule o prijenosu podataka

Zadaća 11: Uključenost u kodekse ponašanja i certificiranje

Suradnja s i savjetovanje s TZP-om:

Zadaća 12: Suradnja s TZP-om

Rješavanje zahtjeva ispitanika:

Zadaća 13: Rješavanje zahtjeva ispitanika

Informiranje i podizanje svijesti:

Zadaća 14: Zadaće informiranja i podizanja svijesti

PRELIMINARNA ZADAĆA:

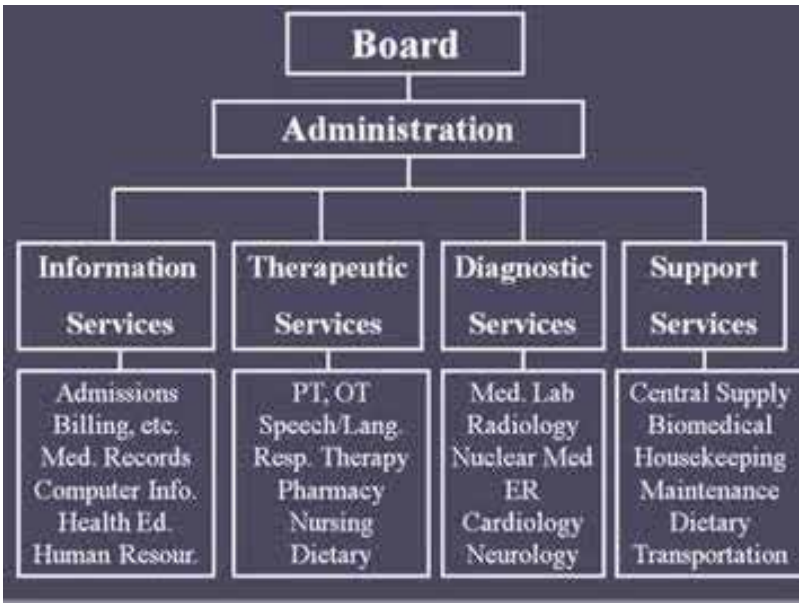
Preliminarna zadaća SZP-a: *istraživanje okoline voditelja obrade i mapiranje aktivnosti postupaka obrade u širem smislu*

SZP može svoje zadaće jedino provesti u odnosu na svojeg poslodavca ako je u potpunosti upoznat/a s (i) **internom** raspodjelom i dodjelom zadaća i odgovornosti u odnosu na (ili koje mogu uključivati) bilo kakvu obradu osobnih podataka; (ii) **vanjskim** poveznicama i dogovorima dotične organizacije s drugim organizacijama; i (iii) **pravnim** okvirima za iste.

Prije poduzimanja svojih drugih glavnih zadaća – izuzev provođenja inicijalnog popisivanja (evidencije) postupaka obrade osobnih podataka, kako je navedeno prvo pod sljedećim naslovom (1. zadaća), što se može provesti paralelno – SZP mora stoga mapirati te interne i vanjske poveznice i linije odgovornosti u odnosu na sve i svaki pojedini postupak obrade osobnih podataka te ih postaviti u širi kontekst uloge i ciljeva svoje organizacije, kao i temeljito se upoznati s relevantnim pravilima.

Radi pojašnjenja **internih** struktura i uloga, SZP mora prije svega pribaviti i proučiti **organigram** unutar svoje organizacije, koji bi uprava trebala dostaviti SZP-u.

PRIMJER: Organigram bolnice



Izvor: *Principles of Health Science*, https://www.youtube.com/watch?v=F-pQEwbAV3Qw

Međutim, organigrami će obično samo identificirati relevantne jedinice i odjele u najopćenitijem smislu: "ljudski resursi (kadrovska)", "financije i računovodstvo", "pravni dio", "odnos s kupcima" itd. (pri čemu mnoga javna tijela usvajaju terminologiju privatnih pravnih osoba, npr. nazivajući tražitelje socijalne skrbi "klijentima/kupcima" ureda za socijalnu skrb). Ovo doista jest korisna početna točka, ali i malo više od samo toga. Pomoću detaljnih razgovora s višim menadžmentom, uključujući službenika(e) za pravni dio i ICT, te, kada je to prikladno, regionalne ili nacionalne urede, SZP bi trebao razjasniti detaljnije za što su točno različite jedinice i odjeli odgovorni, uključujući posebice u koje svrhe svaka od jedinica i odjela treba, odnosno zapravo obrađuje neke osobne podatke; unutar koje arhitekture internih i vanjskih tehnologija se takva obrada vrši; te uključuje li ovo bilo koje vanjske tehnološke usluge ili sredstva (uključujući tzv. *cloud computing* - računarstvo u oblaku). To su mjesta gdje se preliminarno istraživanje preklapa s provođenjem popisivanja

(inventure) postupaka obrade osobnih podataka iz 1. zadaće – ali u preliminarnom stadiju, relevantni postupci obrade osobnih podataka trebaju samo biti identificirani u širem smislu, s referencom na svrhu za svaku takvu obradu te korištene tehnologije. Štoviše, SZP bi trebao u ovoj preliminarnoj fazi također već dobiti inicijalnu ideju o tome koje su to točne **zadaće** i **odgovornosti** svake pojedine jedinice ili odjela u odnosu na svaki postupak obrade osobnih podataka – tj., SZP bi trebao/la identificirati tko je "**vlasnik posla"/"*business owner*"** kod svakog postupka obrade (koristeći terminologiju ENZP-a).

PRIMJERI:[293]

Španjolsko tijelo za zaštitu podataka, AEDP, kao **primjere službenih (zakonski traženih) evidencija osobnih podataka koje vode lokalna tijela** navodi sljedeće:

- Evidencija (registar) stanovništva
- Registar obveznika plaćanja lokalnih poreza
- Registar primatelja povlastica (npr. naknada za stanovanje ili za invaliditet)
- Registar korisnika socijalnih usluga (npr. skrb djece)
- Registar nametnutih novčanih kazni (npr. za pogrešno parkiranje)
- Registar izdanih dozvola i licenci (npr. za otvaranje caffe bara)
- Registar lokalnih policijskih jedinica i policijskih službenika
- Registar korisnika upisanih kod lokalnog ureda za nezaposlene;
- Registar djece uključene u obrazovanje na lokalnoj razini
- Registar pojedinaca kojima su izdane službene isprave (npr. matični podaci o rođenju, sklapanju braka, smrti)
- Registar osoba pokopanih na lokalnim grobljima
- Registar korisnika knjižnica koje vode lokalne vlasti
- Registar pojedinaca koji su se prijavili za primanje obavijesti o kulturnim događanjima Također, kao i:
- Računovodstvo
- Ljudski resursi (kadrovska služba)
- Itd.

Tijelo za zaštitu podataka daje sljedeće **primjere zakona ili propisa koji su osnova za obradu osobnih podataka u odnosu na neke registre osobnih podataka koje vode španjolska lokalna tijela**, navedeno ranije u tekstu:[294]

Registar:	**Zakon/propis koji to propisuje:**
• Evidencija (registar) stanovništva	Zakon o lokalnim registrima stanovništva
• Registar obveznika plaćanja lokalnih poreza	Zakon o lokalnim haciendas
• Podaci o ljudskim resursima	Propisi koji obuhvaćaju ovu djelatnost

U nekim slučajevima, mogu postojati neke druge pravne osnove za postupke obrade, npr.:

Registar:	**Ostale pravne osnove:**
• Registar prijavljenih za kulturna događanja	Privola i lokalni propis
• Registar korisnika lokalnih knjižnica	Ugovor i lokalni propis

293 Na osnovi: Protección de Datos y Administración Local (Zaštita podatka i lokalna uprava) sektorskog vodiča kojeg je izdalo španjolsko tijelo za zaštitu podatka, AEPD, 2017, str. 8 (naš prijevodi i uređivanje), dostupno na: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

294 AEPD, Sectoral Guide on Data Protection and Local Administration (ranija bilješka), str. 11.

Osim toga, važno je da se u ovom stadiju SZP (uz pomoć osoblja iz IT-a i osiguranja) također detaljno upozna s **tehničkim ICT sustavima, – arhitekturom i – politikama svoje organizacije**: koja se računala koriste (ili, tamo gdje se isti još uvijek koriste, ručno vođene zbirke) i uključuju li isti prijenosne i/ili mobilne uređaje (i/ili osobne "vlastite uređaje" dotičnog osoblja – za koje mora biti uspostavljena politika (pravila) "Ponesi svoj vlastiti uređaj"/"Bring Your Own Device [BYOD])"; koriste li se računala ili uređaji kao mrežni ili samo izvan mreže, na samoj lokaciji (on-site) ili također i izvan lokacije (*off-site*); koji sigurnosni softver i enkripcija se koriste, i jesu li isti potpuno ažurirani; kakve su vanjske veze i sadržaji (uključujući korištenje *cloud* poslužitelja, posebno ako su oni smješteni izvan EU/EGP, npr. u SAD-u – u kojem slučaju dotični međusobni dogovori i ugovori o razmjeni podataka moraju biti provjereni); vrše li i koje postupke obrade izvršitelji obrade (u kojem slučaju će trebati preispitati ugovore s njima);[295] koje su postojeće fizičke mjere osiguranja (vrata, prostorije, mrežne i PC lozinke, itd.); postoje li uspostavljene sigurnosne politike (pravila) i osposobljavanje itd. U ovom preliminarnom stadiju, nije nužno pozabaviti se s toliko mnogo pitanja i riješiti ih – ali trebaju biti barem **primijećena, mapirana i evidentirana.**

Nadalje, SZP bi trebao/la pokušati razjasniti sve **vanjske** veze koje njegova/njena organizacija ima s drugim organizacijama. Te se veze općenito javljaju u **dva oblika**: (a) društva/organizacije (sestrinska/osnivačka-matična/društvo kćer) s kojima organizacija SZP-a ima formalne veze, unutar kojih će (u javnom sektoru) obično postojati cjelokupan **hijerarhijski okvir**. Tijelo lokalne vlasti može formalno biti pod izravnom nadležnosti regionalnog tijela, koje je pak nadalje pod kontrolom ili pod nadzorom regionalnog ili saveznog državnog tijela, koje se na najvišoj razini uklapa u širu javnu agenciju/tijelo na državnoj razini, pod nacionalnim ministarstvom. Međutim, postojat će značajne razlike u ovom rasporedu između zemalja, pa čak i unutar jedne države, uključujući pitanja koja se tiču relativne autonomije koju različita tijela imaju, a također i u odnosu na uspostavljanje i vođenje njihovih postupaka obrade osobnih podataka – a to je upravo odgovor na pitanje zašto bi se SZP trebao/la temeljito upoznati s pojedinim rješenjima za svoju dotičnu organizaciju.

Okvir za sva relevantna javna tijela koja pripadaju određenoj hijerarhiji bit će opširno definiran u **formalnom pravu,** u čitavom rasponu razina: ustav, zakoni, zakonski instrumenti (podzakonska, obvezujuća regulativa), ministarske uredbe i upute, kao i u mogućim neobvezujućim **administrativnim rješenjima** ili istima, ali bez zakonske osnove, dogovorima,[296] smjernicama i proklamiranim politikama (*policy statements*) itd. Obrada osobnih podataka od strane organizacije SZP-a može također biti obuhvaćena i **kodeksom ponašanja**, u okviru kojih postoje različite vrste. Opet, SZP bi trebao/la steći što je moguće šire i detaljnije razumijevanje tih pravila i dogovora i kodeksa – kao i o procesima kroz koje se isti usvajaju, primjenjuju i nadziru, te mijenjaju – u mogućoj mjeri; i opet po potrebi uz pomoć službenika iz pravnog odjela u svojoj organizaciji (i/ili polaženjem tečajeva o relevantnim pitanjima ako SZP nije u cijelosti upoznat/a s tim pitanjima prilikom preuzimanja svoje obveze).

Naravno, postojat će drugi SZP-ovi u drugim organizacijama koje pripadaju dotičnoj hijerarhiji – i bit će od presudne važnosti za našeg SZP-a da se u cijelosti poveže s njima, u SZP **mrežu**. U slučaju kada još ne postoji takva mreža, SZP bi trebao raditi na stvaranju iste. Svi SZP-ovi bi naravno trebali uspostaviti **bliske i dobre veze s nacionalnim tijelom za zaštitu podataka (TZP)**, uključujući bilo koje više pozicionirane članove osoblja unutar TZP-a sa specifičnim odgovornostima u odnosu na javna tijela/vrstu javnih tijela kojoj organizacija SZP-a pripada. Rješenja koja je usvojilo francusko tijelo za zaštitu podataka, CNIL, za nacionalnu mrežu SZP-ova, s namjenskim "*extranetom*", dobar je primjer u kojem TZP podržava takvo umrežavanje i interakcije.[297]

295 Španjolsko tijelo za zaštitu podatka, AEPD, kao doprinos u ovom priručniku, navodi kao primjere postupaka obrade koji se često daju vanjskim izvršiteljima od strane lokalnih vlasti (tj., u kojima, u smislu zaštite podataka, obradu vrši izvršitelj obrade): • Obračun plaća • Uništenje dokumentacije ili medija • Upravljanje kamerama za video nadzor • Prikupljanje poreza • Održavanje računalne opreme • Obrada podatka općinskog popisa stanovništva: • Obrada podatka vezano za općinske prireze: • Obrada podataka ljudskih resursa: primjenjivo na reguliranje javne službe. • Pretplata putem usluge koju nudi gradsko vijeće na svojim mrežnim stranicama za primanje obavijesti o kulturnim događanjima. • Upis na burzu za nezaposlene. (AEDP također bilježi računarstvo u oblaku, kako je već navedeno u tekstu.)

296 Ovi ugovori mogu uključivati ugovore između javnih tijela pod kojim jedno javno tijelo obrađuje osobne podatke u ime drugog javnog tijela, tj. nastupa kao izvršitelj obrade za to potonje tijelo. Vidi raspravu u tekstu o voditelj obrade - voditelj obrade, voditelj obrade - izvršitelj obrade i ugovori o prijenosu podataka.

297 Vidi točku 2.3.3, pod naslovom „Formalno osposobljavanje i certificiranje", iznad, i bilješku 228.

Potom postoje poveznice s **vanjskim organizacijama koje su izvan hijerarhije SZP-ove organizacije.** Takve mogu uključivati druga **javna tijela unutar različite hijerarhije** – primjerice, mogu postojati veze između obrazovnih institucija i tijela za socijalnu skrb, ili policije, ili između obrazovnih vlasti u jednoj državi i sličnih organizacija u drugoj. Opet, postojat će (ili bi trebali postojati) **zakoni** koji pokrivaju takve veze s takvim tijelima, ili pak drugi **formalni, obvezujući dogovori i ugovori** (kao što su sporazumi o dijeljenju podataka i ugovori između obrazovnih institucija i organizacija socijalne skrbi). SZP bi i ovdje trebao/la saznati sve detalje o svim takvim dogovorima/sporazumima kad god isti uključuju ili mogu uključivati obradu osobnih podataka – te bi ih doista trebao/la preispitati, kako bi se uvjerio/la odražavaju li na adekvatan način, odnosno potvrđuju li i primjenjuju li zahtjeve propisane GDPR-om, odnosno bilo kojih primjenjivih nacionalnih zakona i pravilnika o zaštiti podataka – kao i općenitijih propisa koji se odnose na zaštitu ljudskih prava.[298] SZP ne može odgovarati za osporavanje manjkavog zakona ili zakonskog dogovora kao takvog, ali bi mogao/la – i trebao/la bi – obavijestiti svojeg poslodavca, kao vjerojatno i nadležni nacionalni TZP o svojem stajalištu da je određeni zakon manjkav.

Ponekad, veze između, kao i suradnja između formalno udaljenih pravnih osoba zasnivaju se na **neformalnim, nejavnim dogovorima.** Međutim, to je problematično s aspekta zaštite podataka. Kako je Radna skupina iz članka 29. iznijela u svojem mišljenju o konceptima voditelja obrade i izvršitelja obrade:[299]

> [Postoji] rastuća tendencija prema organizacijskoj diferencijaciji u najrelevantnijim sektorima. U privatnom sektoru, distribucija financijskih ili drugih rizika dovela je do kontinuirane korporativne diversifikacije, koja je još dodatno ojačana spajanjima i pripajanjima. U javnom sektoru, odvija se slična diversifikacija u kontekstu decentralizacije ili razdvajanje političkih odjela i izvršnih agencija. U oba sektora, postoji rastući naglasak na razvoj lanaca isporuke ili pružanja usluga širom organizacija i za korištenje podugovaranja ili korištenja vanjskih izvršitelja (*outsourcing*) usluga kako bi se uživalo pogodnosti specijalizacije i mogućih ekonomija razmjera. Kao rezultat ovoga, došlo je do rasta različitih usluga, koje nude pružatelji usluga, koji se ne smatraju uvijek odgovornima i pouzdanima. Zbog organizacijskih izbora trgovačkih društava (i njihovih izvođača ili podizvođača) relevantne baze podataka mogu se nalaziti u jednoj ili više država unutar ili izvan Europske unije.

Ovo vodi do poteškoća u odnosu na dijeljenje odgovornosti i dodjeljivanje provedbe kontrole. Radna skupina je rekla da uključene pravne osobe trebaju osigurati "dostatnu jasnoću" o ovoj podjeli odgovornosti i afektivnoj dodjeli (različitih oblika i razina) provedbe kontrole – što u praksi znači da uključene pravne osobe trebaju ***raspraviti*** ova pitanja, ***usuglasiti se*** o tim podjelama i dodjelama odgovornosti, te navedeno ***zabilježiti*** u formi **formalnog dogovora (sporazuma)** koji se može (i na zahtjev, naravno da ga se treba) predati nadležnom tijelu TZP ili TZP-ovima i (možda u pojednostavljenom obliku) ispitanicima, kao i široj javnosti. Kao dio zadaće preliminarnog istraživanja, SZP bi trebao/la ponovo **provjeriti** postoje li takvi formalni dogovori (sporazumi), te ako isti postoje, (a) odražavaju li isti zaista praktične podjele i raspodjele odgovornosti i (b) zadovoljavaju li u potpunosti isti zahtjeve iz GDPR-a. Ako ne postoje formalni dogovori (sporazumi), SZP bi trebao/la **savjetovati** da se hitno treba sastaviti jedan takav (pri čemu SZP treba biti uključen u raspravu o tome, dogovaranje i evidentiranje istoga). Ako postoje samo neformalni dogovori (sporazumi), SZP bi trebao/la **savjetovati** da se isti zamijene formalnima.

Štoviše, kada se veze i dogovori s drugim pravnim osobama svode na ili uključuju dogovore voditelj obrade – voditelj obrade i/ili voditelj obrade – izvršitelj obrade, onda se isti trebaju bazirati na relevantnim (usklađenima s GDPR-om) **ugovorima između voditelja obrade – voditelja obrade i/ili voditelj obrade – izvršitelj obrade;** a kada veze i dogovori s drugim pravnim osobama uključuju prijenos osobnih podataka u države izvan EU/EGP (tzv. "treće zemlje"), prijenosi se trebaju zasnivati na relevantnim (usklađenim s GD-

298 Usp. Europski sud za ljudska prava, presuda u slučaju Copland v. the UK od 3 travnja 2007. g., gdje je Sud smatrao da nejasno sročena odredba u zakonu kojim se jamči široka nadležnost javnoj vlasti u određenom području (in casu, pružanje višeg i daljnjeg obrazovanja) ne predstavlja „zakon" u smislu Europske konvencije o ljudskim pravima: http://hudoc.echr.coe.int/eng?i=001-79996 (posebno vidi st. 47.)

299 RS29, Mišljenje 1/2010 o konceptima „voditelj obrade" i „izvršitelj obrade" (RS169, usvojeno 16. veljače 2010. g.), str. 6, dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

PR-om) **klauzulama o prijenosu podataka** (ili standardne klauzule o zaštiti podataka koje odobri relevantno TZP ili TZP-ovi ili EOZP, ili *ad hoc* klauzule koje su sukladne GDPR-u).

U slučajevima kada takvi ugovori ili klauzule postoje, SZP bi ih trebao/la **preispitati** kako bi provjerio/la jesu li sukladni s GDPR-om, a u slučajevima kada ne postoje takvi ugovori ili klauzule, ali bi trebale postojati, SZP bi trebao/la **savjetovati** da se isti hitno sklope.

Ove zadaće SZP-a u odnosu na formalne dogovore, ugovore između voditelja obrade i voditelja obrade, odnosno voditelja obrade i izvršitelja obrade, te klauzule o prijenosu podataka (i u drugim povezanim aspektima) su dalje raspravljeni pod točkom 3.x, u nastavku. Trenutno, dostatno je napomenuti da bi SZP trebao/la **identificirati** takva pitanja u zadaći preliminarnog istraživanja, kako bi se ta pitanja tek potom rješavala.

Konačno, SZP-ova organizacija će imati **veze s vanjskim (iz privatnog i javnog sektora) dobavljačima roba ili usluga**, u rasponu od obrade podataka dodijeljene vanjskim pružateljima usluga (*outsourcing*), računovodstva i održavanje mrežnih stranica pa sve do opskrbe obroka u kantini, održavanja i popravaka, medicinske i zdravstvene podršku osoblju, itd. Rad koji se tiče obavljanja ovih zadataka zasnivat će se na **ugovorima** (bilo uobičajenim ugovorima građanskog prava ili posebnim javno-privatnim ugovorima). Ovi će ugovori također biti osnova za – i trebali bi stoga posebice to navoditi – bilo koju obradu osobnih podataka od strane ugovornih strana tih ugovora: za prikupljanje relevantnih osobnih podataka radi dijeljenja i korištenja tih podataka, sve do njihovog konačnog uništenja ili brisanja. Ako je druga pravna osoba sama po sebi voditelj obrade, ti ugovori (ili barem elementi relevantni za zaštitu podataka iz tih ugovora) će, u smislu zaštite podataka, predstavljati **ugovore o obradi podataka između dva voditelja obrade podataka**. Ako druga pravna osoba djeluje samo kao izvršitelj obrade za organizaciju SZP-a, ugovor će biti **ugovor između voditelja obrade i izvršitelja obrade**. A ako se prema ugovoru osobni podaci prenose na mjesto izvan EU/EGP-a (tipičan primjer je prijenos na "*cloud*" poslužitelj kojeg održava podizvođač), ovi ugovori predstavljaju **ugovore o prijenosu osobnih podataka**.

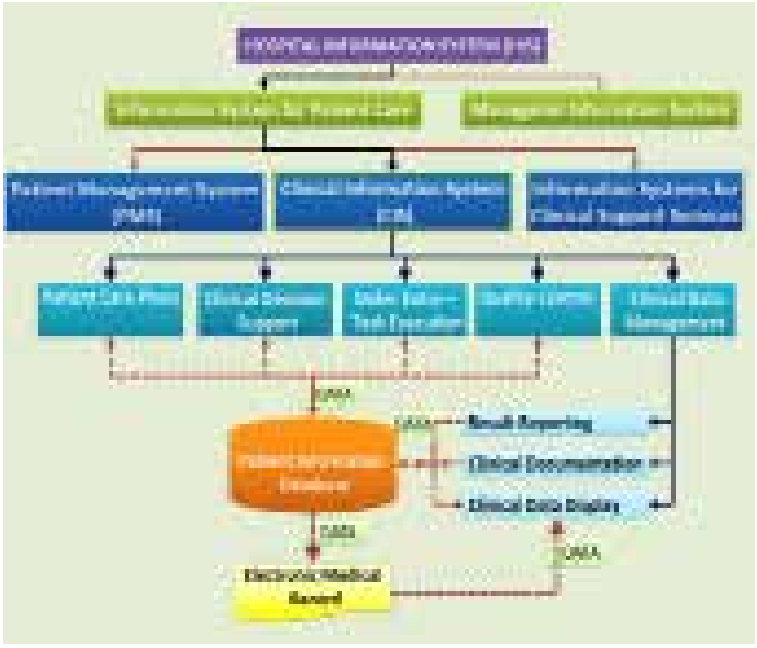
U provođenju preliminarnog istraživanja, SZP bi trebao ponovo **identificirati** postoje li takvi ugovori, a potom, ubrzo nakon provedbe istraživanja, **preispitati** ih, te, u slučajevima gdje takvi ugovori ne postoje ili sadrže manjkavosti u smislu GDPR-a, **savjetovati** da ih se treba sastaviti ili revidirati.

MAPIRANJE AKTIVNOSTI OBRADE ORGANIZACIJE U ŠIREM SMISLU

Kad je SZP već proveo opće istraživanje svoje organizacije (kako je navedeno ranije), SZP će biti u mogućnosti mapirati aktivnosti obrade osobnih podataka organizacije u širem smislu, kao ključni korak prema izradi detaljne evidencije svih onih aktivnosti i svih postupaka obrade pojedinačnih osobnih podataka, što se provodi u 1. zadaći (o čemu se sljedeće raspravlja). To bi trebalo voditi ka izradi tablice kao što je ova u nastavku, autora Dr. Abdollah Salleh, koja iznosi "*Funkcionalne komponente kliničkog informacijskog sustava*" (korišteno u prvoj obuci T4DATA, u prezentaciji talijanskog tijela za zaštitu podataka, *Garante del Privacy*).[300]

300 Luigi Carrozzi, prezentacija za prvi „T4DATA" edukacijski sastanak, lipanj 2018. g., prezentacijski slajdovi na temu „Praktične smjernice za SZP-ove – Evidencija postupaka obrade osobnih podataka"..

PRIMJER: Mapa aktivnosti obrade osobnih podataka organizacije [ovdje: u bolnici]



Izvor: Dr. Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Uzmite u obzir da je ova mapa više povezana s postupcima obrade podataka negoli organigram bolnice, koji je prikazan ranije.

ORGANIZACIJSKE ZADAĆE:

1. ZADAĆA: Stvaranje evidencija aktivnosti obrade osobnih podataka

Uz ograničeni izuzetak o kojem se raspravlja kasnije u tekstu pod tim naslovom, prema članku 30. GDPR-a, svaki voditelj obrade mora "voditi **evidenciju** aktivnosti obrade za koje je odgovoran", navodeći detalje svakog postupka, kao što su ime voditelja obrade (i, može se dodati, "vlasnika posla"/"*business owner*") tog postupka obrade, svrha(e) obrade, kategorije ispitanika, osobni podaci i primatelji itd. Ova obveza vođenja evidencije postupaka obrade blisko je vezana za načelo pouzdanosti [odgovornosti], kako je ranije opisano pod točkom 2.2, omogućavanjem učinkovitog praćenja od strane nadležnog tijela za zaštitu podataka ("nadzorno tijelo") – kako je naglašeno u Uvodnoj odredbi (82) iz GDPR-a:[301]

> *Voditelj obrade ili izvršitelj obrade **treba voditi evidenciju o aktivnostima obrade** pod svojom odgovornošću **radi dokazivanja sukladnosti** s ovom Uredbom.*
>
> Svaki voditelj obrade i izvršitelj obrade **treba imati obvezu surađivati s nadzornim tijelom i omogućiti mu na zahtjev uvid u tu evidenciju** kako bi mu mogla poslužiti za praćenje postupaka obrade.

Drugim riječima, kako navodi talijansko tijelo za zaštitu podataka, *Garante*:[302]

> **[Evidencija je] mjera dokazivanja sukladnosti s GDPR-om**

Pozivanje na "aktivnosti obrade pod odgovornošću [voditelja obrade]" sugerira da evidencija (koju se često također naziva i registar) mora obuhvatiti **sve** takve aktivnosti obrade, a to je doista izrijekom propisano u njemačkoj verziji GDPR-a.[303] Ovo ima smisla također i zato jer, kako *Garante* također naglašava:[304]

> Cjelokupna slika informacijske vrijednosti "osobnih podataka" i povezanih aktivnosti obrade koje pruža registar, je **prvi korak prema pouzdanosti [odgovornosti] s** obzirom da omogućava procjenu rizika za prava i slobode pojedinaca, te za primjenu odgovarajućih tehničkih i organizacijskih mjera za osiguravanje razine sigurnosti odgovarajuće riziku.

Premda, kao i kod većine zahtjeva iz GDPR-a, ovo je formalno obveza voditelja obrade više negoli SZP-a, u praksi će upravo SZP biti ili zadužen za taj posao (u bliskoj suradnji s relevantnim osobljem voditelja obrade) ili će SZP biti osoba u najmanju ruku blisko uključena u taj posao i nadgledati ga. Kao što Radna skupina iz članka 29. (RS29) kaže:[305]

> U praksi, SZP-ovi često stvaraju popis inventara i vode registar aktivnosti obrade na temelju informacija koje su im dostavili različiti odjeli u njihovoj organizaciji zaduženi za obradu osobnih podataka. Ova je praksa ustanovljena sukladno mnogim važećim nacionalnim zakonima prema pravilima o zašti-

301 Luigi Carrozzi, prezentacija na prvom "T4DATA" treningu, lipanj 2018, slajdovi o "*Praktičnim smjernicama za SZP-e – Evidencija aktivnosti obrade*"
302 *Idem*.
303 "*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis **aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.*" (dodan naglasak).
304 Luigi Carrozzi (bilješka 202, iznad) (izvorni naglasak).
305 RS29, Smjernice o SZP-ima (bilješka 209, prethodno u tekstu), odlomak 4.4, *The DPO's role in recordkeeping (Uloga SZP-a kod vođenja evidencije)*, str. 18.

ti podataka primjenjivima na EU institucije i tijela.[306]

Članak 39(1) navodi popis minimuma zadaća koje SZP mora obavljati. Stoga, ništa ne sprječava voditelja obrade ili izvršitelja da dodijele SZP-u zadaću vođenja evidencije o postupcima obrade koji su u okviru odgovornosti voditelja obrade. Takva evidencija treba se smatrati jednim od alata koji omogućava SZP-u provedbu svojih zadaća praćenja sukladnosti, informiranja i savjetovanja voditelja ili izvršitelja obrade.

U svakom slučaju, evidencija čije se vođenje traži prema članku 30. treba se također smatrati alatom za omogućavanje voditelju obrade i nadzornom tijelu, na njihov zahtjev, dobivanja pregleda svih aktivnosti obrade osobnih podataka koje neka organizacija provodi. To je stoga preduvjet za sukladnost, i kao takav, učinkovita mjera pouzdanosti.

Za novog SZP-a, ovo prvenstveno zahtijeva (praćenje) vođenje **popisa** svih aktivnosti obrade dotične organizacije koje mogu obuhvaćati i obradu osobnih podataka i poveznica s drugim organizacijama. Navedeno uključuje razmatranje koji točno podaci predstavljaju takvu vrstu podataka – što nije uvijek jasno.[307]

Početni, osnovni popis može se korisno provesti paralelno sa širim istraživanjem organizacije i njenog operativnog konteksta, u preliminarnoj zadaći (nulta zadaća), kako je opisano ranije. Uz primjenu izuzeća, navedenog kasnije, potom treba uslijediti ***cjeloviti popis***.

Cjeloviti popis treba voditi do stvaranja registra (skup "evidencija") svih aktivnosti obrade osobnih podataka voditelja obrade, spomenutih u članku 30. (kako se obrazlaže malo kasnije u ovom odlomku, pod naslovom "*Sadržaj i struktura zapisa u evidencijama*") – koje potom treba (i nakon preispitivanja i procjene navedenog teksta, u 2. i 3. zadaći) voditi ažurno SZP (ili bi SZP trebao/la barem osigurati da se vode ažurno): vidi daljnji tekst, pod naslovom "*(kontinuirano) Praćenje sukladnosti*", nakon 4. zadaće.

IZUZEĆE:

Članak 30(5) izuzima **poduzeća i organizacije u kojima je zaposleno manje od 250 osoba, a koje samo obrađuju osobne podatke "povremeno"**,[308] od obveze vođenja evidencije svojih aktivnosti obrade osobnih podataka. Međutim, ovo izuzeće ne vrijedi ako:

- će obrada koju provodi poduzeće ili organizacija "*vjerojatno prouzročiti **rizik za prava i slobode ispitanika"*** (primijetite da ovo ne mora biti "visok rizik", kao onaj koji dovodi do potrebe provođenja procjene učinka na zaštitu osobnih podataka (4. zadaća): bilo koji rizik za prava i slobode ispitanika, koliko god malen, zahtijevao bi bilježenje (i preispitivanje) aktivnosti voditelja obrade;
- obrada **nije povremena**; ili
- obrada uključuje **osjetljive podatke ili podatke o kaznenim osudama i kažnjivim djelima**.

U pogledu prvoga, u kontekstu PUZP-a (koji se traži kada postoji "*visok rizik za prava i slobode pojedinaca*": vidjeti 4. zadaću u nastavku), RS29 opisuje izraz "**rizik**" kao:[309]

scenarij koji opisuje događaj i njegove [negativne] posljedice, procijenjen u smislu težine i vjerojatnosti

306 Članak 24(1)(d) Uredba (EC) 45/2001 [izvorna bilješka]
307 Vidi RS29, Mišljenje 4/2007 u odnosu na koncept osobnih podataka (WP136), usvojeno 20. lipnja 2007., dostupno na: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
308 Po našem mišljenju, uvjet da mala organizacija mora samo provoditi obradu osobnih podataka "povremeno" slijedi iz odredbe (raspravljano u tekstu) da se izuzetak ne primjenjuje ako male organizacije ne obrađuju osobne podatke "samo povremeno".
309 RS29 Smjernice o PUZP-ima (bilješka 315, dalje u tekstu), str. 6.

i objasnio je:[310]

> [da se] pozivanje na "**prava i slobode**" ispitanika prvenstveno tiče prava na zaštitu podataka i privatnost, ali može također uključivati i druga temeljna prava, kao što su sloboda govora, sloboda misli, sloboda kretanja, zabrana diskriminacije, pravo na slobodu mišljenja, savjesti i vjeroispovijedi.

U travnju 2018., RS29 izdaje "Dokument o stajalištu" u odnosu na čl. 30(5) GDPR.[311] U predmetnom je istaknuto kako je:

formulacija članka 30(5) jasna u odredbi o postojanju tri vrste obrade na koje se odstupanja ne primjenjuju alternativno (ili), a samo pojavljivanje bilo koje od njih samostalno pokreće obvezu vođenja evidencije aktivnosti obrade. Stoga, iako zapošljavaju manje od 250 zaposlenika, voditelji obrade ili izvršitelji obrade koji se nalaze u poziciji da provode obradu koja bi mogla biti rizična (ne samo visokorizična) za prava ispitanika, ili obrađuju osobne podatke povremeno, ili obrađuju posebne kategorije podataka sukladno čl. 9(1) ili podatke povezane s kaznenim presudama sukladno članku 10., obvezni su voditi evidenciju aktivnosti obrade. Međutim, takve organizacije trebaju voditi evidenciju aktivnosti obrade za vrste obrade navedene u članku 30(5). Na primjer, mala organizacija vjerojatno redovito obrađuje podatke svojih zaposlenika. Posljedično, takva obrada se ne može smatrati "povremenom" i stoga mora biti uključena u evidenciju aktivnosti obrade. Ostale aktivnosti obrade koje su zapravo "povremene", ne moraju biti uključene u evidenciju aktivnosti obrade, pod uvjetom da je malo vjerojatno kako će dovesti do rizika u odnosu na prava i slobode ispitanika te ne uključuju posebne kategorije podataka [tzv. osjetljive podatke] ili osobne podatke povezane s počiniteljima kaznenih djela.

Primjer:

U **Hrvatskoj**, detaljniji podaci o svim državnim službenicima i zaposlenicima u javnim tijelima moraju se prema zakonu unijeti u središnji sustav, *Registar zaposlenih u javnom sektoru*. Ovo također vrijedi i za najmanja javna tijela, kao što su male lokalne zajednice koje moguće zapošljavaju samo vrlo mali broj osoba. Obrada podataka o tih nekoliko zaposlenika od strane te vrlo male zajednice stoga nije "povremena" i ne uživa prednosti izuzeća od vođenja evidencije.

U slučaju sumnje, voditelj obrade treba zatražiti savjet od SZP-a o tim pitanjima – a SZP bi trebao težiti pružiti savjet u smjeru stvaranja cjelokupne evidencije u graničnim slučajevima, umjesto da riskira pozivanje na povredu koju je počinila organizacija radi povrede obveze ugrađene u članku 30(1) – (4).

Bilješke:

1. O pitanju treba li registar aktivnosti obrade osobnih podataka biti učinjen dostupnim svakome (bilo na mreži ili na drugi način) ili pak ne, vidjeti 12. zadaću, "*Zadaće informiranja i podizanja svijesti*".

2. Stvaranje registra kao takvog još ne uključuje procjenu sukladnosti evidentiranih aktivnosti s GDPR-om: to je učinjeno u 2. zadaći – ali, naravno, evidencija treba biti ispravljena i ažurirana kada god se dogode promjene na aktivnostima obrade koje se bilježe u takvoj evidenciji: vidjeti pod "*Praćenje sukladnosti: Kontinuirano ponavljanje Zadaća 1 – 3 (i 4)*", na kraju 4. zadaće (netom prije 5. zadaće).

310 *Idem*, dodan naglasak.

311 RS29, Dokument o stajalištu u odnosu na odstupanja od obveze vođenja evidencije aktivnosti obrade sukladne čl. 30(5) GDPR-, od 19. travnja 2018, dostupno na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045
Dokument o stajalištu nije izričito podržan od strane Europskog odbora za zaštitu podataka kada je isti podržao niz formalnih "Mišljenja" RS29 (EOZP, Odobrenje 1/2018, vidi bilješku 248, iznad), ali se još uvijek može smatrati relevantnim za ovo pitanje.

SADRŽAJ I STRUKTURA UPISA U REGISTAR (EVIDENCIJE):

GDPR razlikuje registre voditelja obrade i onih izvršitelja obrade.

Sadržaj i struktura upisa u registar voditelja obrade (evidencije)

Sukladno članku 30(1) GDPR-a, **evidencija** aktivnosti obrade osobnih podataka *voditelja obrade* treba se sastojati od skupa **evidencija** svake takve aktivnosti; i **svaka takva evidencija mora uključivati sljedeće pojedinosti** (riječi u uglatim zagradama i kurzivu/ukošeni font su dodane):

a. ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
b. svrhe obrade;
c. opis kategorija ispitanika i kategorija osobnih podataka [*uključujući i to pripadaju li bilo koji podaci unutar popisa u "posebne kategorije podataka"/osjetljivi podaci*];
d. kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
e. ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. drugog podstavka, dokumentaciju o odgovarajućim zaštitnim mjerama;
f. ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
g. ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.

Ovaj popis ne uključuje **pravnu osnovu** za obradu relevantnih podataka (članak 6 u odnosu na neosjetljive podatke; članak 9 u odnosu na osjetljive podatke) ili pravne instrumente koji se koriste u ugovorima s izvršiteljima obrade, ili za prijenos podataka – ali su to vrlo važna pitanja u odnosu na bilo koje utvrđivanje zakonitosti i sukladnosti s GDPR-om kod bilo koje aktivnosti obrade podataka, da bi i to trebalo biti zabilježeno u evidenciji, u odnosu na svaku aktivnost obrade osobnih podataka (definirano pozivom na svrhu obrade), uz pravovremenu provjeru valjanosti izjavljene i zabilježene pravne osnove.

OBRAZAC FORMATA OSNOVNE EVIDENCIJE VODITELJA OBRADE PODATAKA O AKTIVNOSTIMA OBRADE PODATAKA312

Primijetite da se odvojena evidencija mora izraditi za svaku zasebnu aktivnost

1. dio – Informacije o voditelju obrade podataka itd.

KONTAKT PODACI **VODITELJA OBRADE**:	Ime, adresa, e-mail, br. telefona
KONTAKT P. **ZAJEDNIČKOG VODITELJA OBRADE**:*	Ime, adresa, e-mail, br. telefona
KONTAKT PODACI **PREDSTAVNIKA**:*	Ime, adresa, e-mail, br. telefona
KONTAKT PODACI **SZP-a**:	Ime, adresa, e-mail, br. telefona
(*) ako je primjenjivo	

312 Prošireno iz predloška obrasca kojeg je predstavio Carrozzi (bilješka 236, prethodno u tekstu) s izmjenama (npr. radije format portret negoli format pejzaž) i upisima o nazivu postupka, pravnoj osnovi za obradu, prikladnim zaštitnim mjerama za prijenose podataka i pojedinostima koje se tiču dodanih tehnologija i sigurnosti (sukladno daljnjim preporukama koje je dao Carrozzi).
NB: Obrazac formulara detaljnije (15 str.) evidencije obrade osobnih podataka je priložen na kraju rasprave o ovoj za

2. dio – Osnovne informacije o aktivnosti obrade osobnih podataka (SZOP aktivnost)[313]

1. Naziv SZOP aktivnosti[314]	
2. Odgovorna jedinica ("vlasnik posla"/ "*business owner*")	
3. Svrha aktivnosti SZOP-a	
4. Kategorije ispitanika	
5. Kategorije osobnih podataka	
6. Uključuje li ovo osjetljive podatke?	
7. Pravna osnova za obradu:* * Usp. čl. 6 GDPR-a za neosjetljive podatke, čl. 9 za osjetljive podatke	
8. Prenose li se podaci u treću zemlju ili međunarodnoj organizaciji?	
9. U slučaju prijenosa navedenih u 2. podstavku članka 49(1) GDPR-a: koje su odgovarajuće zaštitne mjere predviđene?	
10. Rokovi za brisanje	

Sadržaj i struktura upisa u registar izvršitelja obrade (evidencije) [315]

Sukladno članku 30(2) GDPR-a, **evidencija** aktivnosti obrade osobnih podataka *izvršitelja obrade* treba se sastojati od skupa **evidencija** svake takve aktivnosti; i **svaka takva evidencija mora uključivati sljedeće pojedinosti**:

a. ime i kontaktne podatke jednog ili više izvršitelja obrade i svakog voditelja obrade u čije ime izvršitelj obrade djeluje te, ako je primjenjivo, predstavnika voditelja obrade ili izvršitelja obrade te službenika za zaštitu podataka;

b. kategorije obrade koje se obavljaju u ime svakog voditelja obrade;

c. ako je primjenjivo, prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa iz članka 49. stavka 1. točke (h), dokumentaciju o odgovarajućim zaštitnim mjerama;

313 Uzorak tabele gore jedino ima namjeru ilustrirati zahtjeve evidentiranja u širem smislu. Uzorak detaljne evidencije obrade osobnih podataka spomenut u ranijoj bilješci i priložen uz ovu Zadaću traži ključne daljnje pojedinosti, npr. za svaku kategoriju osobnih podataka: svrhu, relventnost i izvor podataka itd….

314 Iz perspektive prava zaštite podatka, bilo koja obrada osobnih podataka je obrada koju je najbolje definirati po osnovi svrhe kojoj služi obrada (kako je zabilježeno pod 2.). Međutim, u mnogim organizacijama, ljudi koji vrše obradu će često imati poseban funkcionalan/interni naziv za obradu – premda se naravno dvije oznake mogu preklapati i biti identične.

315 Primijetite da je sve teže u potpunosti razlikovati izvršitelje obrade od voditelja obrade. Često, pravne osobe koje su prije pružale čiste usluge izvršitelja (djelujući isključivo kako ih uputi voditelj obrade, koji je određivao sredstva i svrhe) sada preuzimaju mnogo više odgovornosti i mogu postati "zajednički voditelji obrade". Ovo je posebno slučaj u odnosu na pružatelje usluga u oblaku – od kojih neki sada već nude "*Artificial Intelligence and Machine Learning (AI/ML) via Machine-Learning-as-a-Service (MLaaS)*", vidi: http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-marketoverview-technology-prospects
Kako je opisano pod *Preliminarnom zadaćom*, dogovori između pravnih osoba uključenih u takve složene aranžmane trebaju biti jasno i pravilno evidentirani. Obrasci za bilježenje relevantnih postupaka obrade trebaju se pregledati i izmijeniti kako bi odgovarali tim (ugovorenim i zabilježenim) međuaranžmanima. Pravne osobe koje su više nego isključivo izvršitelji obrade trebaju koristiti detaljni obrazac spomenut u sljedećoj bilješci.

d. ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.

U nastavku ponovo dajemo obrazac formata primjera evidencije koju izvršitelj obrade treba voditi kako bi udovoljio ovim zahtjevima.

OBRAZAC FORMATA EVIDENCIJE IZVRŠITELJA OBRADE PODATAKA O AKTIVNOSTIMA OBRADE PODATAKA 316

Primijetite da se odvojena evidencija mora izraditi za svaku zasebnu aktivnost za svakog odvojenog voditelja obrade

1.dio – Informacije o izvršitelju obrade podataka i bilo kojem/im podizvršitelju/ima

KONTAKTNI PODACI **IZVRŠITELJA**:	Ime, adresa, e-mail, br. telefona
KONTAKTNI PODACI **SZP-a**:	Ime, adresa, e-mail, br. telefona
KONTAKTNI PODACI **PODIZVRŠITELJA***	Ime, adresa, e-mail, br. telefona
KONTAKTNI PODACI **SZP-a**:	Ime, adresa, e-mail, br. telefona
KONTAKTNI PODACI **PODIZVRŠITELJA***	Ime, adresa, e-mail, br. telefona
KONTAKTNI PODACI **SZP-a**:	Ime, adresa, e-mail, br. telefona
**** Ako je primjenjivo***	

2.dio – Informacije o voditelju obrade specifičnih aktivnosti SZOP-a o kojima se radi

KONTAKT PODACI **VODITELJA OBRADE**:	Ime, adresa, e-mail, br. telefona
KONTAKT P. **ZAJEDNIČKOG VODITELJA OBRADE**:*	Ime, adresa, e-mail, br. telefona
KONTAKT PODACI **ZASTUPNIKA**:*	Ime, adresa, e-mail, br. telefona
KONTAKT PODACI **SZP-a**:	Ime, adresa, e-mail, br. telefona
(*) Ako je primjenjivo	

NB: Odnos između voditelja i izvršitelja obrade, te između izvršitelja obrade i bilo kojeg podizvršitelja, mora se zasnivati na pisanom ugovoru koji udovoljava zahtjevima iz članka 28 GDPR-a. Izvršitelji bi trebali čuvati preslike relevantnih ugovora uz popunjeni obrazac.

316 Ponovo prošireno iz formulara obrasca kojeg je prezentirao Carrozzi (bilješka 236, prethodno u tekstu) s izmjenama.

1.dio – Informacije o aktivnosti obrade osobnih podataka (SZOP aktivnost)

1. Kategorija (vrsta) obrade koja se provodi za voditelja obrade u odnosu na cjelokupnu aktivnost SZP-a, uključujući:	
• kategorije ispitanika;	
• kategorije osobnih podataka; i	
• jesu li uključeni osjetljivi podaci.	
2. Prenose li se podaci u 3. zemlju ili međunarodnoj organizaciji?	
3. U slučaju prijenosa navedenih u 2. podstavku članka 49(1) GDPR-a: koje su odgovarajuće zaštitne mjere predviđene?	
4. Pojedinosti o korištenim sustavima, aplikacijama i procesima *(vrsta elektroničkih datoteka; desktop suite/ centralno upravljana aplikacija / usluga u oblaku (cloud service)/ lokalna mreža;*	
prijenosi podataka itd.) i povezane tehničke i organizacijske (sigurnosne mjere)	
5. Uključuje li obrada upotrebu (a) podizvršitelja? Ukoliko uključuje, navedite potpune podatke i kopiju odgovarajućeg ugovora.	

Sadržaj i struktura evidencije:

SZP treba izgraditi **registar** iz **evidencija** koje primi o svakoj odvojenoj aktivnosti obrade osobnih podataka. Njih je uobičajeno najbolje sortirati prema **organizaciji**, a unutar toga po "vlasniku posla" / "*business owner*"/. Sa svakim pojedinim unosom, SZP bi trebao voditi svu relevantnu dokumentaciju (kako je navedeno u obrascima formulara, ranije u tekstu).

SZP treba zabilježiti u registru kada je svaki od unosa zaprimljen, kada je odnosna aktivnost obrade preispitana (kao što se čini u 2. zadaći, što se opisuje sljedeće), s ishodom takvog preispitivanja i bilo kojim mjerama popravka koje su poduzete; te navesti kada bi aktivnost trebala biti sljedeći puta redovito (npr. jednom godišnje) preispitana.

Priloženo: Obrazac formata detaljne evidencije obrade osobnih podataka[317]

Prilog:

OBRAZAC FORMATA DETALJNE EVIDENCIJE OBRADE OSOBNIH PODATAKA

Molimo koristite odvojeni obrazac za svaku odvojenu aktivnost obrade osobnih podataka

317 Detaljni obrazac evidencije osobnih podatka je također dostavio poljski TZP, *Urząd Ochrony Danych Osobowych* (UODO) na svojim mrežnim stranicama, na poljskom, vidi: https://uodo.gov.pl/pl/123/214 (slijedite prvu poveznicu na dnu stranice.)

NB: Ako smatrate da trebate obrazložiti ili razjasniti neko pitanje, molimo dodajte broj u odgovarajuće polje i priložite stranicu s tim obrazloženjima ili objašnjenjima, uz navođenje tog broja.

I. OPĆENITO: * označava obvezno polje (ako je primjenjivo)

Voditelj obrade: (glavna pravna osoba voditelja obrade)* (Ime, mjesto poslovnog nastana i adresa, broj registracije (matični br.), itd.)	
Povezana društva/pravne osobe (Bilo koje pravne osobe s kojima je voditelj obrade povezan u odnosu na ovu obradu, npr. društva majke/kćeri ili povezana javna tijela; izvršitelji obrade koji su uključeni u ovu obradu)	
Poslovna jedinica: ("vlasnik posla"/ *"business owner"*)* (npr. Kadrovska služba/Ljudski resursi, Računovodstvo, Istraživanje i razvoj, Prodaja, Korisnička podrška)	
Kontakt osoba unutar jedinice:	
PRIMARNA SVRHA POSTUPKA OBRADE OSOBNIH PODATAKA:* ***Molimo opišite što je preciznije moguće***	
Koriste li se osobni podaci ili se isti otkrivaju u bilo koju drugu (sekundarnu) svrhu ili svrhe?* ***Molimo opišite što je preciznije moguće i dodajte poveznicu ili referencu na povezani zapis u evidenciji.***	
Provodi li se ovaj postupak za sve povezane pravne osobe jednako? Ili odvojeno i/ili na različit način za različite pravne osobe?* ***Molimo opišite.*** ***Ako su postupci obrade različiti za različite pravne osobe, molimo koristite odvojene formulare za svaku od njih.***	
Ugrubo gledano, na koliko se pojedinaca (ispitanika) ovaj postupak obrade odnosi (ako je to poznato)?*	[*Upišite broj ili "nije poznato"*]
Datum predaje ovog obrasca SZP-u:*	
Obrazac i postupak obrade preispitao SZP:	[*Da/Ne i datum unosi SZP*]
Predviđeni datum za reviziju/ažuriranje ovog obrasca:	[*Upisuje SZP*]

II. POJEDINOSTI O POSTUPKU OBRADE OSOBNIH PODATAKA:

II.1 Podaci i izvori podataka [NB: Ako je primjenjivo, sva su polja obvezna, osim ako je naznačeno drugačije]

1. Koji osobni podaci ili kategorije osobnih podataka se prikupljaju i koriste za ovaj postupak obrade?	*Označite √ ako je prikladno:*	**Kada, kako i od koga su podaci pribavljeni?** **Npr.:** (ispitanik = I) - DWP, nakon zapošljavanja osobe - I, nakon uključivanja u istraživanje
• Ime(na) i prezime(na)		
• Datum rođenja		
• Kućna adresa		
• Poslovni broj telefona		
• Privatni broj telefona		
• Poslovna email adresa		
• Privatna email adresa		
Dodajte bilo koje daljnje podatke, ispod, ako je primjenjivo:* ** Vidjeti također dolje, na 2, u vezi osjetljivih podataka*		

2.	**Uključuju li podaci koje prikupljate i evidentirate za neki postupak obrade, odnosno otkrivaju li takvi podaci neizravno bilo koje od sljedećih posebnih kategorija osobnih podataka („osjetljivi podaci")?**	Označite √ ako su podaci izrijekom prikupljeni i korišteni za tu aktivnost obrade; Označite √ i dodajte („Neizravno") ako je podatak neizravno otkriven (objasnite u bilješci ako je potrebno)	**Kada su i od koga prikupljeni podaci?** **Npr.: (ispitanik = I)** • **DWP, nakon zapošljavanja osobe** • **I, nakon uključivanja u istraživanje**
	• Rasno ili etničko podrijetlo		
	• Politička mišljenja ili pripadnost stranci		
	• Vjerska ili filozofska uvjerenja		
	• Članstvo u sindikatu		
	• Genetički podaci		
	• Biometrijski podaci		
	• Podaci koji se odnose na zdravlje osobe		
	• Podaci koji se odnose na spolnu orijentaciju ili spolni život osobe		
	• Podaci o kaznenim osudama ili kažnjivim djelima		
	• Nacionalni identifikator* * npr. NI broj nacionalnog osiguranja, porezni broj		
	• Podaci o dugovanjima/ kreditnoj sposobnosti		
	• Podaci o maloljetnicima		
3.	**Ako je ovo poznato ili utvrđeno: Koliko dugo se (posebni i drugi) podaci zadržavaju? Što se potom događa?*** * Navedite razdoblje ili događaj, npr. „7 godina" ili „Po isteku 5 godina nakon prestanka zaposlenja". Također objasnite što se događa s podacima, npr. brisanje/uništenje ili anonimizacija. NB: Ako su rokovi zadržavanja različiti za različite podatke, molimo to navedite.		

II.2 Otkrivanje podataka

	4. Kojim trećim stranama se koji od gore navedenih podataka otkrivaju? I u koje svrhe? **NB: Ovo se primjenjuje i na podatke koji se čine dostupnima, posebno izravno, putem mreže (*online*)** ***Vezano za* otkrivanja koja uključuju prijenose u treće zemlje, vidjeti dalje u nastavku, pod II.5.**	**Treća strana primatelj, te mjesto i država poslovnog nastana:**	**Svrha(e) otkrivanja:**
	• Ime(na) i prezime(na)		
	• Datum rođenja		
	• Kućna adresa		
	• Poslovni broj telefona		
	• Privatni broj telefona		
	• Poslovna email adresa		
	• Privatna email adresa		
	• Rasno ili etničko podrijetlo		
	• Politička mišljenja ili pripadnost stranci		
	• Vjerska ili filozofska uvjerenja		
	• Članstvo u sindikatu		
	• Genetički podaci		
	• Biometrijski podaci		
	• Podaci koji se odnose na zdravlje osobe		
	• Podaci koji se odnose na spolnu orijentaciju ili spolni život osobe		
	• Podaci o kaznenim osudama ili kažnjivim djelima		
	• Nacionalni identifikator* * npr. NI broj nacionalnog osiguranja, porezni broj		
	• Podaci o dugovanjima/ kreditnoj sposobnosti		

	• Podaci o maloljetnicima		

II.3 Pravna osnova za obradu podataka

5.	**Po kojoj se pravnoj osnovi obrađuju osobni podaci?** NB: Ako postoje različite pravne osnove za različite podatke ili za različite (primarne, sekundarne ili nove, nevezano) svrhe, molimo navedite to (ako je potrebno kopiranjem i lijepljenjem/copy&paste ranijih popisa podataka dolje u tekst, uz pomicanje različitih pravnih osnova u drugi stupac).	Označite relevantnu pravnu osnovu i dati pojašnjenje u sljedeći stupac kao relevantan	**Pojašnjenje:**
	• Ispitanik je dao privolu za obradu podataka **NB: Vidjeti također QQs 6 – 9, ispod.**		
	• Obrada je nužna za ugovor između Vaše organizacije i ispitanika **(Ili da bi se poduzeli koraci na zahtjev ispitanika prije sklapanja ugovora – npr. dobivanje preporuka)**		
	• Obrada je nužna radi poštivanja pravnih obveza koje obvezuju Vašu organizaciju * **Npr. radno ili porezno pravo – molimo navedite dotično pravo**		
	• Obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe		
	• Obrada je nužna za izvršavanje zadaće od javnog interesa * *** Molimo navedite pravnu osnovu zadaće (obično, zakon)**		
	• Obrada je nužna pri izvršavanju službene ovlasti *** Molimo navedite pravnu osnovu zadaće (obično, zakon)**		
	• Obrada je nužna za potrebe legitimnih interesa Vaše organizacije (ili treće pravne osobe), ali interesi ispitanika nisu jači od interesa obrade **Npr. marketing prema Vašim vlastitim klijentima, ili sprječavanje prijevare – molimo navedite poimence.**		
	PRIVOLA – dodatni detalji:		

6.	**Ako se podaci obrađuju temeljem privole ispitanika, kako i kada se ova privola pribavlja?** **NB: Ako se privola daje na papiru ili u elektroničkom obliku, molimo pridružite presliku relevantnog teksta/poveznicu**	
7.	**Kakav dokaz se čuva o danoj privoli?** **Npr. čuvaju li se preslike u papirnom obliku ili kao zapisi elektroničke privole?**	
8.	**Koliko se dugo ovaj dokaz zadržava?**	
9.	**Ako u kontekstu ugovora Vaša organizacija traži više podataka negoli je potrebno za svrhe ugovora, je li ispitanik informiran da ne mora pružiti dodatne podatke?** **NB: Ili navedite "nije dostupno", ili, ako ovo jest primjenjivo, priložite presliku relevantnog teksta/poveznice**	

II.4 Informiranje ispitanika [NB: Ove informacije nisu obvezne, ali su korisne kod procjene i revidiranja internih pravila (politika) zaštite podataka]

10. Jesu li ispitanici informirani o sljedećem? **Ako da, kada i kako?**	*Navedite Da/Ne (ili "nije dostupno")* **NB: Ako je to relevantno, možete reći "Očigledno proizlazi iz konteksta" i/ili "Ispitanik je već imao tu informaciju"**	Objasnite kada i kako je to učinjeno **Molimo priložite preslike bilo kojih obavijesti o informacijama ili poveznice**
• Da je Vaša organizacija voditelj obrade aktivnosti obrade osobnih podataka?		
• Detalji o Vašoj organizaciji (npr. naziv/ime i matični/reg. broj)?		
• Ako je primjenjivo, detalji o Vašem zastupniku u EU?		
• Kontaktni podaci SZP-a?		
• Glavna svrha obrade?		
• Bilo koja daljnja svrha radi koje Vaša organizacija želi (ili može željeti) obrađivati podatke?		
• Ako podaci nisu dobiveni izravno od ispitanika, izvor ili izvori podataka, te jesu li isti uključivali javno dostupne izvore (kao što su javni registri)?		
• Primatelji ili kategorije primatelja podataka? **NB: Usp. Q4, iznad**		
• Jesu li podaci (treba li ih se) prenijeti u državu izvan EU/EGP-a (*npr., na cloud poslužitelj u SAD-u*)? **NB: Ovo se također primjenjuje i na podatke koji su učinjeni dostupnima (posebno izravno, preko mreže/online) pravnim osobama u zemljama izvan EU/EGP-a.**		
• Ako se podaci tako prenose, koje su zaštitne mjere primijenjene, te gdje ispitanici mogu dobiti preslike istih? **NB: Zaštitne mjere mogu se predvidjeti u ugovorima o prijenosu podataka ili putem kodeksa o privatnosti ili pečata privatnosti (EuroPriSe).**		

	• Koliko dugo će se podaci zadržati?		
	• O njihovim pravima da zatraže pristup, ispravak ili brisanje podataka; pravo zatražiti da se ograniči obrada njihovih podataka; pravo uložiti prigovor na obradu?		
	• O njihovom pravu da podnesu prigovor nadležnom Tijelu za zaštitu podataka?		
11.	• **Ako se svi ili dio podataka obrađuju na osnovi privole, jesu li ispitanici obaviješteni o sljedećem?**		
	• Da oni mogu povući svoju privolu u bilo koje doba (i kako to učiniti) (bez da to utječe na zakonitost prethodne obrade)?		
12.	**Ako je pružanje podataka zakonska ili ugovorna obveza (ili uvjet nužan za sklapanje ugovora), jesu li ispitanici obaviješteni o sljedećem?**	*Navedite Da/Ne (ili "nije dostupno")* **NB: Ako je to relevantno, možete reći "Očigledno proizlazi iz konteksta" i/ili "Ispitanik je već imao tu informaciju"**	Objasnite kada i kako je to učinjeno **Molimo priložite preslike bilo kojih obavijesti o informacijama ili poveznice**
	• Traži li se od njih da pruže podatke te koje su posljedice ako ih oni ne pruže?		
13.	**Ako se svi ili dio podataka obrađuju po osnovi kriterija "legitimnih interesa", jesu li ispitanici informirani o tome o kojem se legitimnom interesu u tom slučaju radi?**		Molimo iznesite kratak sažetak kriterija primijenjenih u testu ravnoteže provedenom u odnosu na temeljna prava i slobode ispitanika prema članku 6(1)f GDPR-a.
14.	**Ako će ispitanici biti podložni automatiziranom donošenju odluka ili profiliranju, jesu li obaviješteni o sljedećem?**		Molimo navedite kratak sažetak logike korištene kod automatiziranog donošenja odluka ili profiliranja.
	• Da će se takvo donošenje odluka ili profiliranje odviti?		
	• U širokom (ali smislenom) smislu, koja je "logika" primijenjena?		

• Koji je značaj automatiziranog donošenja odluka ili profiliranja te koje su predviđene posljedice takvog donošenja odluka ili profiliranja?		

II.5 Prekogranični protok podataka [NB: Upis u polju 17 nije obvezan, ali opet je koristan za internu procjenu]

15. Prenose li se ikoji osobni podaci u treću zemlju [tj. zemlju izvan EU/EGP-a] (ili u sektor u trećoj zemlji) ili međunarodnoj organizaciji za koju se smatra da pruža "primjerenu" razinu zaštite sukladno čl. 45 GDPR-a?	*Navedite Da/ne i zemlju/e o kojoj/kojima se radi.* *Ako se radi o prijenosu samo nekih, ali ne svih podataka, navedite to za svaku kategoriju podataka.*	*Objasnite svrhu prijenosa, npr.: kao dio vlastitih djelatnosti Vaše organizacije (npr. kod korištenja softvera u oblaku/cloud), ili kao dio otkrivanja podataka trećoj strani (molimo navedite tu/e treću/e stranu/e)*
• Ime(na) i prezime(na)		
• Datum rođenja		
• Kućna adresa		
• Poslovni broj telefona		
• Privatni broj telefona		
• Poslovna email adresa		
• Privatna email adresa		
• Rasno ili etničko podrijetlo		
• Politička mišljenja ili pripadnost stranci		
• Vjerska ili filozofska uvjerenja		
• Članstvo u sindikatu		
• Genetički podaci		
• Biometrijski podaci		
• Podaci koji se odnose na zdravlje osobe		
• Podaci koji se odnose na spolnu orijentaciju ili spolni život osobe		
• Podaci o kaznenim osudama ili kažnjivim djelima		
• Nacionalni identifikator* * npr. NI broj nacionalnog osiguranja, porezni broj		
• Podaci o dugovanjima/ kreditnoj sposobnosti		

• Podaci o maloljetnicima		

16. Jesu li bilo koji od podataka preneseni u treću zemlju [tj., izvan EU/EGP-a] (ili neki sektor u trećoj zemlji) ili međunarodnoj organizaciji za koju se ne smatra da pruža "primjerenu" razinu zaštite prema čl. 45 GDPR-a?	*Navedite Da/ne i zemlju/e o kojoj/kojima se radi.* *Ako se radi o prijenosu samo nekih, ali ne svih podataka, navedite to za svaku kategoriju podataka.*	*Objasnite svrhu prijenosa, npr.: kao dio vlastitih djelatnosti Vaše organizacije (npr. kod korištenja softvera u oblaku/cloud), ili kao dio otkrivanja podataka trećoj strani (molimo navedite tu/e treću/e stranu/e)*	*Koja zaštitna mjera ili derogacija podupire prijenos?* *Molimo navedite broj sukladno popisu u* ****Bilješci*** *dolje u tekstu i priložite presliku bilo kojeg relevantnog dokumenta*
NB: *Ako se podaci prenose zbog različitih svrha različitim primateljima u različitim zemljama, molimo odgovorite na pitanja odvojeno za svaki kontekst prijenosa.*			
• Ime(na) i prezime(na)			
• Datum rođenja			
• Kućna adresa			
• Poslovni broj telefona			
• Privatni broj telefona			
• Poslovna email adresa			
• Privatna email adresa			
• Rasno ili etničko podrijetlo			
• Politička mišljenja ili pripadnost stranci			
• Vjerska ili filozofska uvjerenja			
• Članstvo u sindikatu			
• Genetički podaci			
• Biometrijski podaci			
• Podaci koji se odnose na zdravlje osobe			
• Podaci koji se odnose na spolnu orijentaciju ili spolni život osobe			
• Podaci o kaznenim osudama ili kažnjivim djelima			
• Nacionalni identifikator* * npr. NI broj nacionalnog osiguranja, porezni broj			
• Podaci o dugovanjima/ kreditnoj sposobnosti			

• Podaci o maloljetnicima			

*** BILJEŠKA:** Prema GDPR-u, prijenosi u zemlje za koje se ne smatra da pružaju "primjerenu" zaštitu, mogu se odviti samo ako postoje "odgovarajuće zaštitne mjere", kako je navedeno u lijevom stupcu, ispod, ili ako se primjenjuje derogacija (odstupanje), kako je navedeno u desnom stupcu.

Zaštitne mjere prema čl. 46 GDPR-a: 1. Međunarodni instrument između tijela javnih vlasti; 2. Obvezujuća korporativna pravila (OKP); 3. Odobrene standardne klauzule o prijenosu podataka; 4. Kodeks ponašanja; 5. Certificiranje; 6. Odobrene *ad hoc* klauzule	Derogacije (odstupanja) sukladno čl. 49 GDPR-a, ako nisu dostupne zaštitne mjere sukladno čl. 46 (vidjeti Smjernice EOZP-a u tom smislu: restriktivna primjena i tumačenje su obvezni): 7. Privola; 8. Ugovor između voditelja obrade i ispitanika; 9. Ugovor između voditelja obrade i treće strane; 10. Nužnost iz važnih razloga javnog interesa; 11. Nužnost za pravne zahtjeve; 12. Nužno za zaštitu životno važnih interesa ispitanika ili drugih osoba; 13. Prijenos se obavlja iz registra dostupnog javnosti.

17.	**Postoje li pravila za rješavanje bilo koje presude suda ili pravorijeka arbitražnog tribunala, kao i bilo koje odluke upravnog tijela treće zemlje, koja se može uručiti voditelju obrade ili bilo kojem izvršitelju obrade, a kojom se zahtijeva od voditelja ili izvršitelja da prenesu ili otkriju osobne podatke?** (Usp. čl. 48 GDPR-a)	*Navedite Da/Ne, a ako ste naveli Da, molimo priložite presliku smjernice.*

III. SIGURNOST I POVJERLJIVOST

NB: Ako se odgovori na donja pitanja razlikuju za različite podatke, molimo odgovorite na njih odvojeno za svaki odvojeni niz podataka.	*Molimo navedite detalje:*
Čuvaju li se osobni podaci navedeni pod II.1 u papirnatom ili elektroničkom formatu? Ako su u papirnatom, čuvaju li se u strukturiranoj ručno vođenoj evidenciji (spis s osobnim podacima)?	
Gdje se (fizički) podaci čuvaju? (U Vašim uredima? Na poslužiteljima kod glavnog voditelja obrade? Na poslužiteljima povezane organizacije? Na poslužiteljima treće strane (npr. pružatelj usluga u *oblaku/Cloud Service Provider*)?	
Koje mjere postoje za zaštitu od neovlaštenog pristupa fizičkim prostorijama gdje su podaci pohranjeni/gdje su dostupni? Postoje li pravila sigurnosti podataka kojima se regulira ovo pitanje? *(Ako da, molimo priložite primjerak)*	
Koji se hardver koristi kod obrade podataka? Tko je odgovoran za upravljanje i sigurnost ovog hardvera?	
Jesu li (bilo koji od) podataka pohranjeni na odvojivim medijima/uređajima)? Koji su to mediji/uređaji? U čijem se posjedu isti nalaze?	
Može li itko od osoba koje imaju pristup podacima koristiti osobne uređaje za pristupanje ili obradu podataka? Ako da, postoji li BYOD ("Donesi svoj uređaj") politika (pravila) u tom slučaju? *Molimo priložite primjerak politike (pravila).*	

Jesu li sve osobe ovlaštene za pristupanje osobnim podacima pod obvezom čuvanja povjerljivosti (bilo po osnovi zakonske obveze ili profesionalne grupe normi ili po osnovi ugovora)? *Molimo navedite detalje ili priložite primjerke bilo kojih relevantnih pravila ili ugovornih klauzula.*	
Koji se softver, tj. aplikacija/e koristi/e kod obrade podataka? (npr. desktop MS Office paket, centralno upravljana aplikacija, *cloud* usluga - pohrana u oblaku itd.)	
• Upravlja li se ovim softverom lokalno ili centralno? Ako je odgovor centralno, tko je centralna pravna osoba? Ako to niste Vi, postoji li formalni dogovor između te pravne osobe i Vaše organizacije u pogledu korištenja softvera? *Molimo priložite primjerak ovog dogovora.*	
• Koristi li softver tzv. "*cloud*"? Ako da, tko je pružatelj *cloud* usluga, te gdje je pravno sjedište tog pružatelja usluge? Te gdje se fizički nalazi/e *cloud* poslužitelj/i? Jesu li podaci na *cloud* poslužitelju u cijelosti enkriptirani? Kako je to učinjeno (tj. korištenjem koje tehnologije enkripcije)? *Molimo priložite primjerak ugovora po osnovi kojeg se ova obrada odvija.*	
• Tko je odgovoran (tj. tko ima "admin" ovlasti) u odnosu na taj softver? (Vi? Netko drugi unutar Vaše organizacije? Netko u centralnoj pravnoj osobi s kojom ste povezani? Neka druga osoba?)	
Prenose li se podaci u bilo koje doba/pod bilo kojim okolnostima elektronički na drugi medij, sustav ili uređaj?	
Ako se prenose elektronički, vrši li se to: • Putem mreže? Ako da, jesu li podaci enkriptirani? Kako je to učinjeno (tj. korištenjem koje tehnologije enkripcije)? • Pomoću FTP-a? Kako je to osigurano? • Pomoću VPN-a? Kako je to osigurano? Ostalo – *molimo precizirajte.*	

2. ZADAĆA: *Preispitivanje postupaka obrade osobnih podataka*

Za SZP, nakon kreiranja registra postupaka obrade osobnih podataka unutar svoje organizacije (1. zadaća), sljedeći je korak provođenje dubinskog **preispitivanja** svih zabilježenih postupaka obrade osobnih podataka, kako bi se provjerilo ispunjavaju li isti zahtjeve GDPR-a u svim relevantnim aspektima, uključujući u pogledu sljedećeg:

- specifikacija svrhe i ograničenje svrhe;
- valjanost bilo koje privole (i postojanje dokumentiranog dokaza o danoj privoli) ili prihvatljivost bilo koje druge pravne osnove za obradu;
- obrađeni osobni podaci i njihova relevantnost, te nužnost u odnosu na navedenu(e) svrhu(e);
- kvaliteta podataka (točnost, ažurnost i dr. podataka, kao i minimizacija podataka i pseudonimizacija);
- informacije pružene ispitaniku na vlastitu inicijativu voditelja obrade (bilo kada su se podaci prikupljali od ispitanika ili na drugi način, bilo na zahtjev – također u odnosu na podatke prikupljene od posjetitelja mrežnih stranica);
- vremensko razdoblje (rok) na koji se podaci zadržavaju u formi koju je moguće
- identificirati, te bilo koje informacije u smislu deidentifikacije;
- tehnička, organizacijska i fizička sigurnost podataka (uključujući ograničenje fizičkog pristupa i ograničenje tehničkog pristupa [korisničko ime, lozinke, politika za PIN-ove, itd.], enkripcija, itd.);
- prekogranični prijenosi podataka (i zakonski, te drugi ugovorni ili ostali dogovori u vezi istih);
- itd.

U svjetlu nalaza o gore navedenim pitanjima, SZP bi trebao/la biti u mogućnosti **procijeniti**:

- može li se za postupak obrade **kao cjelinu** reći da je sukladan s prevladavajućim načelom zakonitosti i poštenosti [pravednosti].

(Primijetite da je ova procjena sukladnosti s GDPR-om odvojena i različita od procjene rizika, opisane dalje u tekstu kao 3. zadaća).

Evidencije postupka obrade individualnih osobnih podataka kreirane u 1. zadaći (posebice ako su kreirane u detaljnijem formatu)[318] bi trebale tvoriti osnovu preispitivanja, u smislu da će dovesti SZP do toga da se zapita i odgovori na relevantna pitanja koja posebice uključuju sljedeće:

- Je li dostatno jasno koja je pravna osoba **voditelj obrade** postupaka obrade osobnih podataka, te ako su uključene bilo koje druge pravne osobe, koji je njihov odnosni
- status (npr. ***zajednički voditelji obrade***, ***izvršitelji obrade***, ili odvojeni voditelj obrade ***treća strana***)? Ako ovo nije očigledno, postoje li **formalni dogovori** koji pojašnjavaju ova pitanja (usp. 1. zadaću, ranije u tekstu)?
- Je li dostatno jasno koja poslovna jedinica je "**vlasnik posla" ("business owner")** u odnosu na postupak obrade osobnih podataka (tj. koja ima svakodnevnu *de facto* odgovornost za obradu)? Je li ovo sadržano u **formalnom dokumentu** (npr. izričite upute voditelja obrade poslovnoj jedinici)?
- Je li **svrha**, odnosno jesu li **svrhe**, postupka obrade osobnih podataka navedene dostatno preciznim terminima? Gdje (tj. u kojoj vrsti **dokumenta**)? Ako se osobni podaci korišteni u postupku obrade koriste za više od jedne svrhe, koja je ***primarna svrha*** i što je ili što su ***sekundarna(e) svrha(e)***? Jesu li te sekundarne svrhe ***kompatibilne*** s primarnom svrhom, ili su to odvojene svrhe?

  NB: Kod procjene sukladnosti bilo koje obrade za bilo koju sekundarnu svrhu s primarnom svrhom, SZP mora uzeti u obzir pitanja navedena u članku 6(4) GDPR.

  Jesu li sve svrhe za koje se osobni podaci obrađuju u potpunosti opravdane i zakonite?

318 Kao što je predviđeno u formatu uzorka detaljnog zapisa obrade osobnih podataka priloženog zadatku 1.

- Jesu li osobni podaci koji se obrađuju **adekvatni**, **relevantni** i **nužni** za primarnu svrhu? Kako se osigurava da oni budu i ostanu **točni** i **ažurni** za ovu svrhu, i koji dogovori su postignuti kako bi se ovo osiguralo i kako bi se ***ispravile*** ili ***ažurirale*** ili ***izbrisale*** netočne ili zastarjele informacije?

  Jesu li poduzete mjere adekvatne i dostatne? Bi li se ista svrha mogla postići s manjim rizikom za privatnost i druga prava pojedinaca o kojima se u tom slučaju radi?

- Koji se osobni podaci koriste ili otkrivaju za bilo koje sekundarne svrhe ili doista nove, nepovezane svrhe (obično, trećoj strani)? Jesu li osobni podaci koji se obrađuju **primjereni**, **relevantni** i **nužni** za takve sekundarne ili nove, nepovezane svrhe? (Ako se svi prikupljeni podaci za jednu [primarnu] svrhu otkrivaju bez razmišljanja za neku/bilo koju sekundarnu svrhu ili svrhe ili za novu, nevezanu svrhu, oni, ili neki od njih, mogu itekako biti pretjerani za tu sekundarnu ili nepovezanu svrhu ili te sekundarne ili nepovezane svrhe. Je li ovo uzeto u obzir?)

  NB: Usp. Detaljan formular obrade osobnih podataka, pod točkom II.2.

  Jesu li sve sekundarne svrhe za koje se osobni podaci obrađuju potpuno opravdane i zakonite?

- Kako se osigurava da su podaci koji se koriste ili otkrivaju za sekundarne ili nove, nepovezane svrhe **točni** i **ažurni** za te sekundarne ili nove svrhe u doba prvog korištenja ili otkrivanja za te svrhe, i kakvi su dogovori postignuti da se osigura da isti *ostanu* **točni** i **ažurni** nakon prvog korištenja ili otkrivanja te da se isti ***isprave*** ili ***ažuriraju*** ili ***izbrišu*** čim i kada isti postanu netočni ili zastarjeli? Jesu li relevantne mjere primjerene i dostatne?

  NB: Ako se podaci koriste ili otkrivaju za više od jedne sekundarne ili nove svrhe, ova pitanja trebaju biti odgovorena odvojeno za svako odvojeno sekundarno ili novo korištenje ili otkrivanje.

- **Kada, kako, od koga i u kojem obliku** se **koji** osobni podaci pribavljaju? Npr.: ispitanik, neki odjel državne vlasti, (bivši) poslodavac itd.; npr. u papirnatom obliku, elektroničkim prijenosom itd.

  NB: Ovo pitanje treba biti odgovoreno i za **neosjetljive** i **osjetljive podatke**, a ako se drugačiji podaci dobivaju od različitih izvora, to treba biti naznačeno. Usp. Detaljan obrazac obrade osobnih podataka, pod točkom II.1 i II.2.

  Jesu li ti izvori odgovarajući? Bi li se za neke podatke koji su pribavljeni od trećih strana možda moglo radije pitati same ispitanike?

- **Koliko dugo** se osobni (neosjetljivi i osjetljivi) podaci **zadržavaju**? Što se događa istekom tog roka? (Npr.: ***brisanje***, ***uništenje***, ***anonimizacija*** – ili ***pseudonimizacija*** – ali primijetite da potonje znači da se podaci i dalje zadržavaju u obliku kojim ih se može identificirati).[319] Ako se podaci zadržavaju u anonimiziranom ili pseudonimiziranom obliku, ***zašto*** se to čini? (Npr. radi istraživačke svrhe ili svrhe arhiviranja? Ako je tako, obrada za tu svrhu bi trebala biti odvojeno procijenjena u pogledu sukladnosti s GDPR-om.)

  NB: Rok zadržavanja može biti definiran kao specifično vrijeme ili kao događaj, npr., "7 godina" ili "Po isteku 5 godina nakon prestanka zaposlenja". Primijetite da postoje **formalni standardi** o preporučenim metodama brisanja/uništenja podataka za različite kategorije podataka i nosača podata-

319 Primijetite da prema GDPR-u (kao i prema Direktivi o zaštiti podataka iz 1995.), može se reći da su osobni podaci anonimizirani samo ako ih se više ne može povezati s određenim pojedincem od strane bilo koga – tj. ne misli se samo na voditelja obrade (ali isto tako, npr. od kolega, rođaka ili prijatelja koji bi mogli pronaći podatke ako budu objavljeni u navodno neidentificiranom obliku na internetu ili odbačenom papiru). U tom smislu, SZP-ovi bi trebali biti svjesni da sve više i više podataka koji se mogu činiti "neosobnim" ili za koje se kaže da su "anonimizirani" mogu sve više biti (ponovno)povezani s određenim pojedincima. Posebice, podatke u navodno "anonimnim" "Big Data" nizovima podataka se često neočekivano, i zabrinjavajuće, može ponovno identificirati, posebno ako različiti nizovi podataka budu povezani ili "upareni". Nadalje, čak i ako se koriste doista neosobni nizovi podataka za stvaranje "profila" (bilo tipičnog potrošača određenog proizvoda, ili tipičnih pacijenata, ili tipičnih kriminalaca ili terorista), a ti se profili potom primijene na nizove podataka kako bi se izdvojili pojedinci koji zadovoljavaju uvjete profila – tada i ta obrada također može vrlo ozbiljno utjecati na te pojedince, kojima se može uskratiti osiguranje, ili posao, ili pristup zrakoplovu ili čak državi (ili još gore) na temelju učinkovito nespornih algoritama. Vidi: Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, izvještaj za Savjetodavni odbor Vijeća Europe o zaštiti podataka, lipanj 2015., dokument Vijeća Europe T-PD(2015)11, odlomak I.iii, *The dangers inherent in data mining and profiling*, dostupno na: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

ka.[320] SZP bi trebao/la provjeriti je li se to poštovalo (posebno što se tiče osjetljivih podataka bilo u smislu zakonitosti zaštite podataka ili u širem socijalnom ili političkom smislu).

Jesu li rokovi zadržavanja podataka prikladni? Ili su predugi? Jesu li mjere brisanja/uništenja podataka sukladne nacionalnim i međunarodnim standardima? Ako se podaci zadržavaju preko uobičajenih rokova zadržavanja u anonimiziranom ili pseudonimiziranom obliku: (i) je li to prikladno u smislu svrhe produženog zadržavanja? Bi li se podaci zadržani u pseudonimiziranom obliku mogli zadržati u potpuno anonimiziranom obliku, ali i dalje biti dostatni za tu posebnu svrhu? Koliko je istinita bilo koja tvrdnja da su bilo koji podaci "anonimizirani"? (Primijetite da se potpuna anonimizacija sve teže postiže, posebno s velikim nizovima podataka, a tim više ako je dopušteno nizove podataka uparivati ili povezivati s drugim nizovima podataka.)

- Kojim **trećim stranama** se koji od gornjih podataka **otkrivaju**? I **za koje svrhe**? Jesu li podaci koji se otkrivaju ***primjereni***, ***relevantni*** i ***nužni*** za te svrhe, jesu li ***točni*** i ***ažurirani***, a ako jesu, kako se osigurava da takvi i ostanu?

  NB: Odgovori na ova pitanja mogu se djelomično preklapati s odgovorima na ranija pitanja, prije u tekstu.
- Na kojoj(im) **pravnoj/im osnovi/ama** se osobni podaci obrađuju?

  NB: Za neosjetljive podatke, pravna osnova mora biti jedna od onih navedenih u članku 6. GDPR-a, a za osjetljive podatke, jedna od onih navedenih u članku 9. GDPR-a.

  Primijetite da se osnova "legitimni interes" za obradu (čl. 6(1)(f)) ne primjenjuje na obradu bilo kojih podataka – uključujući neosjetljive podatke – od strane tijela javnih vlasti pri izvršavanju njihovih zadaća (čl. 6(1), posljednja rečenica) i na njih se ne može oslanjati ni jedan voditelj obrade, bilo da je iz javnog ili privatnog sektora, radi obrade osjetljivih podataka (usp. čl. 9).

  Štoviše, ako se obrada temelji na članku 6(1)(c) ili (e) ("obrada [koja] je nužna radi poštivanja pravnih obveza voditelja obrade", "obrada [koja] je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade"), to se mora temeljiti na pravu Unije ili države članice EU-a (čl. 6(3)). Ako je išta od ovoga navedeno kao pravna osnova, SZP mora provjeriti zadovoljava li odgovarajući zakon zahtjeve iznesene u članku 6(3) GDPR-a.

  Je li pravna osnova koju se navodi kao osnovu odgovarajuća obradi? Jesu li relevantni uvjeti za primjenu pravne osnove zadovoljeni (npr., što se tiče privole, kako se opisuje dalje u tekstu)?

  Primijetite da se pravna osnova obrade za primarnu svrhu može razlikovati od pravne osnove za bilo koju obradu (uključujući korištenje ili otkrivanje) bilo kojih podataka za bilo koju(e)

- US National Security Agency/Central Security Service, Media Destruction Guidance,na https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

  sekundarnu(e) ili novu(e), nepovezanu(e) svrhu(e) – a valjanost pravne osnove na koju se poziva mora biti procijenjena odvojeno za svaku od tih svrha.

- Ako se podaci obrađuju po osnovi **privole** ispitanika:
- ***kako i kada*** se privola pribavlja (npr. u papirnatom obliku ili elektroničkom, izravnim pitanjem ili traženjem pojedinca da označi kvadratić)?[321]

320 Vidi primjer:
DIN German Institute for Standardization, Office machines - Destruction of data carriers, DIN 66399, listopad 2012.
NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, prosinac 2014, na http://dx.doi.org/10.6028/NIST.SP.800-88r1

321 Primijetite da jednostavna izjava na mrežnim stranicama koja navodi: "*Ako nastavite koristiti mrežne stranice, Vi dajete svoju privolu da prikupljamo i koristimo Vaše osobne podatke*" više nije dostatna da predstavlja valjanu privolu prema GDPR-u. Ne samo da je nedostatna informacija o korištenju podataka – što čini "privolu" nevaljalom jer to nije "informirani pristanak". Ali također, upitno je predstavlja li nastavak korištenja mrežnih stranica sam po sebi "*nedvosmislenu naznaku želja ispitanika*" na koju je dao/la privolu (usp. definiciju privole u čl. 4(11)

- koji se ***dokaz*** čuva o tome da je dana privola (npr. papirnati primjerci, elektronički zapis (*log*)?
- kako i koliko dugo se ovaj dokaz ***zadržava***?
- ako Vaša organizacija u kontekstu ugovora traži više podataka negoli je potrebno za ugovor, je li ispitaniku ***rečeno da ne mora pružiti dodatne podatke***?
- Jesu li **ispitanici informirani** o svim pitanjima o kojima ih se treba obavijestiti (vidjeti članak 13 i 14 GDPR-a, kako se vidi u detaljnom obrascu za obradu osobnih podataka, u točki II.4), a ako da, kada i kako?

  Jesu li pružene sve relevantne informacije? Je li to učinjeno u najboljem formatu? U najbolje vrijeme? Razlikuju li se jasno obvezna polja od neobaveznih?
- Jesu li bilo koji podaci **preneseni u treću [tj. izvan EU/EGP-a] zemlju** (ili sektor u trećoj zemlji) ili **međunarodnoj organizaciji** za koju *se* smatra da pruža "primjerenu" razinu zaštite prema čl. 45 GDPR-a?

  Obuhvaća li doista relevantna odluka o primjerenosti obradu? Je li i dalje valjana (usp. Utvrđenje SEU-a da je odluka o primjerenosti "Safe Harbor" bila nevaljana)?
- Jesu li bilo koji podaci **preneseni u treću [tj. izvan EU/EGP-a] zemlju** (ili sektor u trećoj zemlji) ili **međunarodnoj organizaciji** koja se **ne** smatra da pruža "primjerenu" razinu zaštite prema čl. 45 GDPR-a? Ako da, koje zaštitne mjere ili izuzeća su podloga prijenosa?

  NB: Sukladno GDPR-u, prijenosi u zemlje za koje se ne smatra da pružaju "primjerenu" zaštitu mogu se dogoditi ako *ili* postoje "**odgovarajuće zaštitne mjere**", kako su navedene u čl. 46. GDPR-a, *ili* ako se primjenjuje **izuzeće**, kako je navedeno u čl. 48 GDPR-a (usp. odlomak II.5 u detaljnom obrascu obrade osobnih podataka, pitanje 16).

  Je/jesu li spomenuta(e) zaštitna(e) mjera(e) ili izuzeće(a) točni? Udovoljava/ju li zahtjevima ispisane u relevantnom članku (čl. 46 ili 48)?
- Postoje li pravila za postupanje s bilo kojom presudom/pravorijekom suda/tribunala, te bilo kojom odlukom upravnog tijela treće zemlje, koja može biti uručena voditelju obrade ili bilo kojem izvršitelju, pri čemu se traži od voditelja obrade ili izvršitelja da prenese ili otkrije osobne podatke?

  NB: Sukladno članku 48. GDPR-a, presude i odluke trećih zemalja "mogu biti priznate ili izvršive na bilo koji način samo ako se temelje na nekom međunarodnom sporazumu, poput ugovora o uzajamnoj pravnoj pomoći, koji je na snazi između treće zemlje koja je podnijela zahtjev i Unije ili države članice, ne dovodeći u pitanje druge razloge za prijenos u skladu s ovim poglavljem". Ovo je teško za procjenu za vlasnike posla i mnoge voditelje i izvršitelje obrade, te bi trebale postojati smjernice o tome kako vlasnici posla i voditelji, odnosno izvršitelji trebaju postupati ako su suočeni s takvom presudom ili odlukom. U najmanju ruku, izvršitelji i vlasnici posla bi trebali odmah uputiti predmet na najvišu razinu uprave unutar voditelja obrade i SZP-u.

  Ako postoje relevantne smjernice, je li adekvatno (npr. ako je isto usvojeno prije cjelovite primjene GDPR-a, možda ne spominje uključivanja SZP-a u predmet, s obzirom da možda nije još bilo SZP-a kada su se sastavljale smjernice)? Ako još nema smjernica o ovome, treba ih žurno sastaviti, uz savjetovanje sa SZP-om vezano za sadržaj istih.
- Koje formalne, organizacijske, praktične i tehničke mjere postoje kako bi se osigurala sigurnost i povjerljivost podataka?

  NB: Prema članku 32. GDPR-a, voditelji obrade i izvršitelji moraju primijeniti "odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik[e]" koje

GDPR).

obrada predstavlja za prava i slobode fizičkih osoba (uključujući posebice ispitanike). Članak navodi različite mjere kao što su pseudonimizacija i enkripcija, klauzule o povjerljivosti, tehničke mjere za osiguranje integriteta, dostupnosti i otpornosti korištenih sustava, te vraćanja sposobnosti.

Ovo pitanje će biti detaljnije razrađeno u 3. zadaći (procjena rizika). Međutim, **inicijalni pregled** poduzetih mjera (odnosno mjera koje nisu poduzete) bi već trebao biti dobiven u kontekstu 2. zadaće, kako bi se dalo **preliminarno upozorenje** o tome jesu li poduzete mjere "prikladne" u svjetlu odredbe "uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca" (kako je sadržano u članku 32.

Mnoge (premda ne sve) mjere obuhvaćene su priznatim međunarodnim standardima, kao što su ovi navedeni u nastavku. Međutim, treba naglasiti da iste ne pokrivaju uvijek sva relevantna pitanja, npr. imaju tendenciju fokusirati se na sigurnost više nego li na minimizaciju ili ograničenje svrhe.[322]

Premda je tako, SZP-ovi bi trebali biti upoznati sa standardima kao što su ovi – i provjeriti radi utvrđivanja jesu li ih njihov TZP ili EOZP komentirali (na pozitivan ili negativan način, ili pak s dodacima):[323]

- ISO/IEC 27001:2013 Kodeks prakse za informacijsku sigurnost
- ISO/IEC 29100 – Informacijska tehnologija — Tehnike sigurnosti — Okvir
- privatnosti
- ISO/IEC 27018 – Kodeks prakse zaštite podataka koji se mogu identificirati (PII) u javnim oblacima koji djeluju kao PII izvršitelji obrade
- ISO/IEC 29134 – Smjernice o procjeni učinka na zaštitu podataka (PUZP)
- ISO/IEC 29151 – Kodeks prakse za zaštitu informacija po kojima se može
- identificirati osoba
- JIS 15001:2006 – Zahtjevi sustava upravljanja zaštitom osobnih podataka
- BS 10012:2017 – Specifikacija za sustav upravljanja osobnim podacima
- Daljnji standardi su u pripremi:
- ISO 20889 – Tehnike poboljšanja privatnosti kod de-identifikacije podataka
- ISO 29184 – Mrežne obavijesti o privatnosti i privola
- ISO 27552 Poboljšanje ISO/IEC 27001 za upravljanje privatnosti – Zahtjevi Novi naslov: Proširenje ISO/IEC 27001 i ISO/IEC 27002 za upravljanje privatnim informacijama – Zahtjevi i smjernice
- UNI referentna praksa – Smjernice za upravljanje osobnim podacima u ICT okolinama prema GDPR-u

Ako se koristi "oblak" kod obrade, treba također razmotriti jesu li također uzeta u obzir pitanja koja su navedena u "Povjerljivi oblak – Profil zaštite podataka za usluge u oblaku (TCDP)", smjernicama koje su izdane unutar pilot projekta kojeg je poduprla njemačka vlada, "Certifikacija zaštite podataka za usluge u oblaku"/"*Data Protection Certification for Cloud Services*" (premda se iste i dalje pozivaju na njemački Savezni zakon o zaštiti podataka iz vremena prije GDPR-a, a ne na sami GDPR).[324]

U ovom stadiju, SZP bi trebao provjeriti jesu li voditelj obrade i/ili vlasnici posla svjesni gore navedenih standarda, te jesu li usmjereni na njihovu primjenu, a ako jesu, postoje li certifikacije u tom

322 Prije nekoliko godina, TZP-ovi su primijetili da ISO isprava o sigurnosti koja je obuhvaćala PIN kodove nije navodila broj i prirodu znakova koji se trebaju koristiti. Od tad, TZP-ovi imaju pravilo biti u interakciji što je moguće više s ISO grupama čije aktivnosti se odnose na bilo kojeg ispitanika.
323 Izvor: Alessandra de Marco, prezentacijski slajd za prvi edukacijski sastanak "T4DATA", lipanj 2018., slajdovi na temu "*Postojeći standardi (za sigurnost i privatnost)*" i "*Standardi (za privatnost) još nisu finalizirani*".
324 Vidi:
https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (vidi posebice popis standarda na str. 14-16). Verzija dostupna u doba pisanja rada (v.1.0) datira iz rujna 2016., ali se autori nadaju da – nakon stvaranja računovodstvenih standarda i procedura certifikacije ojačanih GDPR-om – "*TCDP certifikacije će biti pretvorene u certifikacije sukladno Općoj Uredbi za usluge u oblaku*". (str. 7). Usp. također raspravu o čimbenicima rizika itd. koje je prepoznao Europski nadzornik za zaštitu podatka u odnosu na usluge u oblaku, o čemu se govori kod 3. zadaće, dalje u tekstu.

smislu. Pitanje o tome poštuju li se isti u cijelosti, ili bi se doista trebali poštovati, može se detaljnije razmotriti u 3. zadaći (procjena rizika).

Ovaj pregled je prva instanca SZP-ove funkcije "Trajnog praćenja sukladnosti" (dalje opisano pod tim naslovom nakon 4. zadaće).

Ako je, u bilo kojem smislu, SZP mišljenja da postupak obrade osobnih podataka ne udovoljava bilo kojem od zahtjeva GDPR-a, SZP mora **savjetovati** relevantnu interno nadležnu osobu ili osobe o manjkavostima te predložiti radnje popravka (uključujući čak i zaustavljanje obrade u cijelosti, ako je to potrebno). U slučaju da se ne postupi po tom savjetu, SZP bi trebao/la uputiti pitanje vodećoj upravi (vidjeti u nastavku, pod "*Savjetodavne zadaće*").

Zamijetite da je ovaj općeniti pregled postupaka obrade odvojeno pitanje od situacije pojave povrede osobnih podataka, kako se obrazlaže vezano za 6. zadaću ("*Rješavanje povreda osobnih podataka*"): kako se tamo objašnjava, te povrede bi trebale *odmah* biti prijavljene najvišim razinama uprave.

SZP treba voditi cjelovitu **evidenciju** svih svojih preispitivanja i procjena, kao i o takvim danim savjetima.

3. ZADAĆA: *Procjenjivanje rizika nametnutih postupcima obrade osobnih podataka*

Kako je opisano pod točkom 2.2.1, iznad, GDPR nameće opću obvezu *voditeljima obrade* da "[uzimajući] u obzir prirodu, opseg, kontekst i svrhe obrade, kao i **rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca**" koje se nameću kod svakog postupka obrade osobnih podataka, te obvezu "[provesti] odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom" (čl. 24(1); usp. također čl. 25(1)).

SZP, također:

> pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade (čl. 39(2)).

Poštivanje ovih zahtjeva zahtijeva da se utvrde relevantni rizici. To treba učiniti vezano za vođenje popisa postupaka obrade osobnih podataka i kreiranja registra tih postupaka (1. zadaća) i, posebice, uz preispitivanje tih postupaka (2. zadaća).

GDPR izrijekom ne zahtijeva uključenost SZP-a u bilo koju opću procjenu rizika: uredba propisuje takvo uključivanje SZP-a samo vezano za dublju procjenu učinka na zaštitu podataka (čl. 35(2) – vidjeti 4. zadaću, ispod). Međutim, u praksi bilo bi nadasve uputno (najblaže rečeno) uključiti SZP-a također i u ovu općenitiju procjenu rizika. Doista, u praksi, procjena će često ovisiti o gledištima SZP-a.

Treba primijetiti da rizici koje treba procijeniti nisu samo sigurnosni rizici u užem smislu – tj., vjerojatnost i učinak **povrede osobnih podataka**[325] – već štoviše rizici za **prava i slobode ispitanika (i drugih pojedinaca)** koji se mogu nametnuti uslijed postupaka obrade. Ovo uključuje ne samo njihova opća prava na privatnost i privatan život kao i njihova specifična prava ispitanika, već također uključuje, ovisno o slučaju, njihova prava na slobodu izražavanja, slobodu kretanja, zabranu diskriminacije, slobodu od autoritarne vlasti i pravo ostati u demokratskom društvu bez nepriličnog nadziranja vlastite države ili drugih država, kao i pravo na učinkovite pravne lijekove. Ovaj je koncept širok.[326]

325 "**Povreda osobnih podataka**" je definirana u GDPR-u kao: "kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani" (čl. 4(12)). Vidi 6. zadaću, dalje u tekstu.

326 Usp. rasprave o značenju riječi "rizik" i "visoki rizik" pod 1. zadaćom (pod naslovom "*Izuzeća*") i 4. zadaćom.

Opća procjena rizika treba također uzeti u obzir zaključke iz 2. zadaće. Primjerice, ako je utvrđeno da je određeni postupak obrade bio, sam po sebi, zakonit (tj. imao je valjanu pravnu osnovu i služio je legitimnom interesu), ali da su prikupljeni nebitni i pretjerani podaci te su čuvani za dotičnu svrhu, suprotno načelu "minimizacije podataka" – tada se može reći da to predstavlja "rizik" samo po sebi, tj. da bi se nebitni i pretjerani podaci koristili pogrešno. U tom slučaju, odgovarajuća mjera za izbjegavanje tog rizika bila bi prestanak prikupljanja

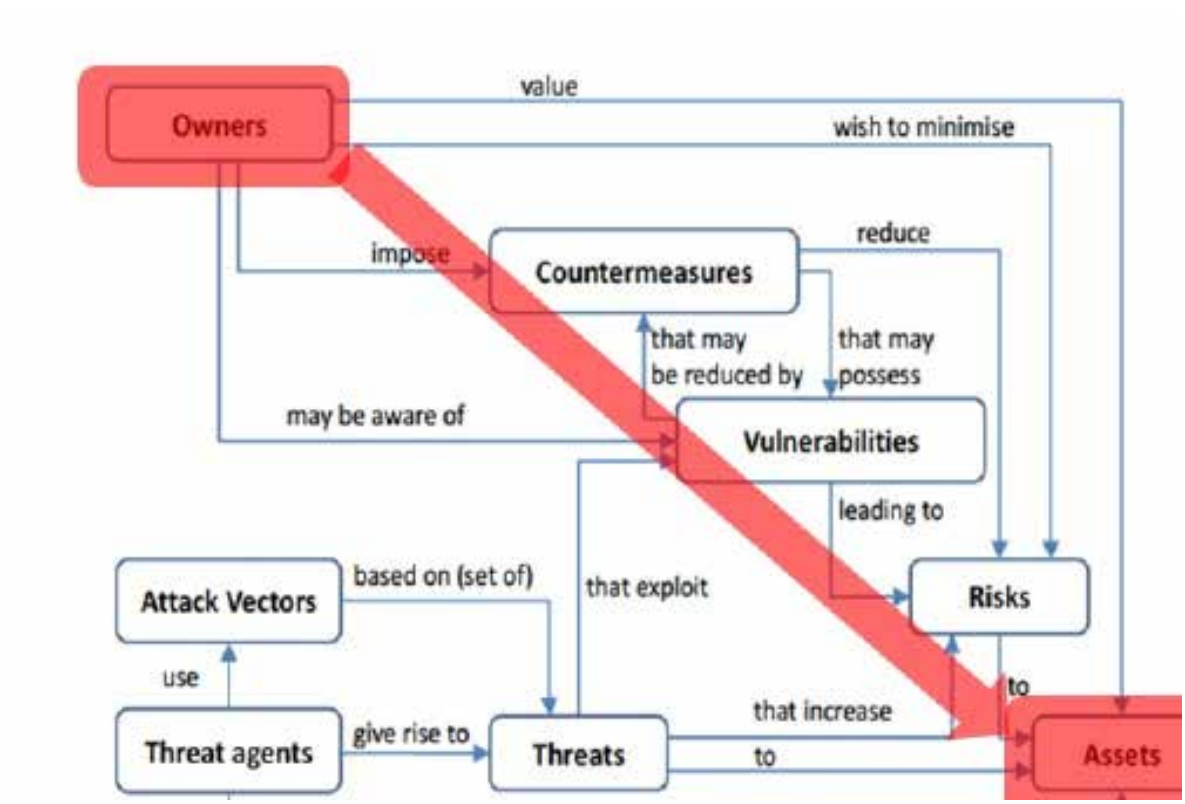
nebitnih i nepotrebnih podataka, kao i brisanje bilo kojih takvih podataka koji se već čuvaju. Drugi bi primjer bio korištenje podataka po kojima se i dalje može identificirati osoba u statističkoj obradi koja se može provesti pomoću pseudonimizacije ili čak potpune anonimizacije podataka – u tom slučaju, odgovarajuća mjera bila bi osigurati da se korišteni podaci pravilno (ozbiljno) pseudonimiziraju ili (po mogućnosti) u cijelosti anonimiziraju.

Sve ovo naglašava da za opći pregled (2. zadaća) i procjenu rizika (trenutna 3. zadaća), voditelj obrade – u praksi, SZP – mora pažljivo razmotriti **sve aspekte svakog odvojenog postupka obrade osobnih podataka i svaku funkciju**.

Kako predlaže talijansko tijelo za zaštitu podataka, *Garante*, korisno je slijediti pristup koji je usvojila ENISA (Agencija EU-a za mrežnu i informacijsku sigurnost), koja pak nadograđuje široko prihvaćeni standard ISO 27005: "*Prijetnje iskorištavaju ranjivosti imovine i time uzrokuju štetu za organizaciju*"; i razmotriti detaljnije **rizik** koji je sastavljen od sljedećih ***elemenata***:

Imovina (Ranjivosti, Kontrole), **Prijetnja** (Profil napadača - Threat Agent Profile, Vjerojatnost - Likelihood i **Impact (učinak)**.

Elementi rizika i njihovi odnosi mogu se tada ilustrirati kako slijedi:



Izvor: ENISA Threat Landscape Report 2016, Slika 4: Elementi rizika i njihovi odnosi prema ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.
Vidi i izvještaj iz 2017., https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Kako također iznosi *Garante*, **valjana procjena rizika uključuje četiri koraka**:[327]

1. Definicija postupka obrade i njegov kontekst;
2. Razumijevanje i procjena učinka;
3. Definicija mogućih prijetnji i procjena njihove vjerojatnosti (vjerojatnost pojave prijetnje) ;
4. Procjena rizika (kombiniranjem vjerojatnosti pojave prijetnje i učinka) ;

Prvo navedeno (definiranje postupka obrade i njegovog konteksta) je učinjeno u 1. i 2. zadaći, iznad u tekstu.

Drugi korak uključuje **definiranje različitih razina učinka** – što može razumno ostati na četiri razine, kako slijedi:[328]

RAZINA učinka	Opis
Niska	Pojedinci se mogu susresti s manjim neugodnostima, koje mogu savladati bez ikakvog problema (vrijeme provedeno na ponovni unos podataka, "gnjavaža", nelagoda itd.
Srednja	Pojedinci se mogu susresti sa značajnim neugodnostima, koje će uspjeti savladati usprkos nekim poteškoćama (dodatni troškovi, uskrata pristupa poslovnim uslugama, strah, manjak razumijevanja, stres, manji fizički nedostaci itd.).
Visoka	Pojedinci se mogu suočiti sa značajnim posljedicama, koje bi trebali moći savladati usprkos ozbiljnim poteškoćama (zlouporaba novčanih sredstava, stavljanje na crnu listu od strane financijskih institucija, štete na imovini, gubitak zaposlenja, poziv na sud, pogoršanje zdravlja itd.).
Vrlo visoka	Pojedinci koji se mogu susresti sa značajnim, ili čak nepovratnim posljedicama, koje ne mogu savladati (nemogućnost rada, dugotrajne psihološke ili fizičke bolesti, smrt itd.).

Garante bilježi četiri glavna područja procjene u smislu **sigurnosti podataka**, tj.:

A. Mrežni i tehnički resursi (hardverska oprema i softver)
B. Procesi/procedure vezani za postupak obrade podataka
C. Različite strane i osobe uključene u postupak obrade podataka
D. Poslovni sektor i volumen obrade.

Za svako područje procjene, postavlja se **pet pitanja**, pri čemu pozitivan odgovor ukazuje na rizik, kako je navedeno u tablici na sljedećoj strani.[329]

Osoba koja procjenjuje sigurnosni rizik može, iz tih odgovora, potom izračunati **vjerojatnost pojave prijetnje**, kako je navedeno u dvije tablice pod tim naslovom, nakon tablice, na sljedećoj strani.

Taj se rezultat tada može kombinirati s rezultatom učinka kako bi se došlo do **rezultata cjelokupnog rizika**, kako je navedeno u tablici nakon ovih.

ČETIRI GLAVNA PODRUČJA PROCJENE U SMISLU SIGURNOSTI PODATAKA:

327 Giuseppe d'Acquisto, prezentacijski slajd za prvi edukacijski sastanak "T4DATA" o sigurnosti podataka, lipanj 2018., na temu "*Procjena rizika (fokus na sigurnosti)*".
328 *Idem*, prezentacijski slajd na temu "*Razumijevanje i procjenjivanje učinka*".
329 *Idem*, prezentacijski slajdovi o svakoj od ovih četiri glavna područja procjene, s daljnjim objašnjenjem o tome zašto pozitivan odgovor na pitanje u svakom slučaju predstavlja sigurnosni rizik.

A. Mrežni i tehnički resursi:	B. Procesi i procedure	C. Uključene strane i osobe	D. Poslovni sektor i volumen
1. Je li bilo koji dio obrade osobnih podataka proveden putem mreže (internet)?	**6.** Jesu li uloge i odgovornosti u pogledu obrade osobnih podataka nejasne ili nisu jasno definirane?	**11.** Provodi li obradu osobnih podataka nedefiniran broj zaposlenika?	**16.** Smatrate li Vaš poslovni sektor kao sektor sklon kibernetičkim napadima?
2. Je li moguće osigurati pristup internom sustavu obrade osobnih podataka putem mreže/interneta (npr. za određene korisnike ili grupe korisnika)?	**7.** Je li prihvatljivo korištenje mreže, sustava i fizičkih resursa unutar organizacije višeznačno ili nije jasno definirano?	**12.** Provodi li se bilo koji dio obrade osobnih podataka putem podizvođača/treće strane (izvršitelj obrade)?	**17.** Je li Vaša organizacija pretrpjela bilo koji kibernetički napad ili drugu vrstu povrede sigurnosti u posljednje dvije godine?
3. Je li sustav obrade osobnih podataka međupovezan s drugim vanjskim ili internim (u odnosu na Vašu organizaciju) IT sustavom ili uslugom?	**8.** Je li zaposlenicima dopušteno donijeti i koristiti vlastite uređaje kako bi se povezali sa sustavom obrade osobnih podataka?	**13.** Jesu li obveze strana/osoba uključenih u obradu osobnih podataka višeznačni ili nisu jasno navedeni?	**18.** Jeste li dobili bilo kakve obavijesti i/ili pritužbe u pogledu sigurnosti IT sustava (koji se koristi za obradu osobnih podataka) tijekom prošle godine?
4. Mogu li neovlašteni pojedinci lako pristupiti okolini u kojoj se obrađuju podaci?	**9.** Je li zaposlenicima dopušteno prenositi, pohranjivati ili na drugi način obrađivati osobne podatke izvan prostorija organizacije?	**14.** Je li osoblje uključeno u obradu osobnih podataka upoznato ili nije s pitanjima sigurnosti informacija?	**19.** Tiče li se postupak obrade velikog broja pojedinaca i/ili osobnih podataka?
5. Je li sustav obrade osobnih podataka dizajniran, primijenjen ili održavan bez praćenja relevantne najbolje prakse?	**10.** Mogu li se aktivnosti obrade osobnih podataka provoditi bez stvaranja elektroničkih zapisa (log)?	**15.** Zanemaruju li osobe/strane uključene u postupke obrade osobnih podataka sigurnu pohranu i/ili uništavanje osobnih podataka?	**20.** Postoje li bilo kakve najbolje prakse u smislu sigurnosti, specifične za Vaš poslovni sektor, a koje nisu adekvatno primjenjivane?

VJEROJATNOST POJAVE PRIJETNJE (1):

Područje procjene:	Broj odgovora "da"	Razina	Bodovi
A. Resursi mreže i tehnički resursi:	0 – 1	Malena	**1**
	2 – 3	Srednja	**2**
	4 – 5	Velika	**3**
B. Procesi i procedure	0 – 1	Malena	**1**
	2 – 3	Srednja	**2**
	4 – 5	Velika	**3**
C. Uključene strane i osobe	0 – 1	Malena	**1**
	2 – 3	Srednja	**2**
	4 – 5	Velika	**3**
D. Poslovni sektor i volumen	0 – 1	Malena	**1**
	2 – 3	Srednja	**2**
	4 – 5	Velika	**3**

Gornji bodovi mogu se unijeti u sljedeću sažetu tablicu:

VJEROJATNOST POJAVE PRIJETNJE (2):

Cjelokupan ZBROJ bodova:	*RAZINA VJEROJATNOSTI pojave prijetnje:*
4 – 5	***Malena***
6 – 8	***Srednja***
9 – 12	***Visoka***

Na koncu, ovi rezultati se onda mogu kombinirati s rezultatima "Razine učinka" navedenima u prvoj tablici gore, da bi se prikazao cjelokupan rizik, kako slijedi:

PROCJENA CJELOKUPNOG RIZIKA:

		RAZINA UČINKA		
		Malena	**Srednja**	**Velika/vrlo velika**
VJEROJATNOST POJAVE PRIJETNJE	**Mala**			
	Srednja			
	Velika			

Legenda:

Malen rizik *Srednji rizik* *Velik rizik*

NAPOMINJEMO, MEĐUTIM da se gore navedena shema procjene rizika uglavnom odnosi na **rizike sigurnosti podataka**.

Ovo je zasigurno jedna bitna kategorija rizika koju treba procijeniti i kojom se treba pozabaviti – i to ne samo jednom, već na kontinuiranoj osnovi, jer rizici mogu s vremenom evoluirati i mutirati. Usp. bilješku pod naslovom: "*Praćenje sukladnosti: Kontinuirano ponavljanje Zadaća 1 – 3 (i 4)*" na kraju razrade 4. zadaće, netom prije rasprave o 5. zadaći, dalje u tekstu.

Međutim, GDPR se također, općenitije, poziva na "**rizik[e] za prava i slobode pojedinaca**" (vidi članke 34, 35 i 36). Prvi članak, članak 34., očigledno prihvaća da povrede podataka, kao takve, mogu rezultirati takvim rizicima, te nameće važna pravila o tome kako ih riješiti, što se obrazlaže u zadaćama 4. (PUZP-e), 7. (istražna zadaća), 12 (suradnja s TZP-om) i 14 (informiranje i podizanje svijesti).

Međutim, treba primijetiti da **"rizici za prava i slobode pojedinaca" ne nastaju samo iz povreda podataka**. Sama Uredba propisuje u članku 35(1) da "*visok rizik*" ove vrste može proisteći, posebice, iz:

- sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca;
- opsežne obrade posebnih kategorija osobnih podataka iz članka 9. stavka 1. ili podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.; ili
- sustavnog praćenja javno dostupnog područja u velikoj mjeri.

U tim slučajevima, *upravo zato što takvi postupci obrade predstavljaju **inherentno visoke rizike** za prava i slobode pojedinaca,* potrebna je procjena učinka na zaštitu podataka (u nekim slučajevima se mora konzultirati nadležno nadzorno tijelo ili tijela), kako se raspravlja u okviru sljedeće zadaće.

Podrobnije, automatizirano donošenje odluka, uključujući izradu profila može dovesti do **nepravednih odluka** (jer nitko nije u potpunosti jednak bilo kojem drugom pojedincu te ni jedan sustav ne bi, nadamo se, mogao znati sve o nekoj osobi) ili nedemokratskih odluka s **diskriminatornim, a ipak neosporivim ishodima**;[330] korištenje osjetljivih podataka može također dovesti do **diskriminacije** (neovisno je li namjeravana ili ne);[331] korištenje čak naoko bezopasnih podataka o izvršenim prodajama može otkriti intimne zdravstvene probleme ili trudnoću);[332] a sustavno praćenje osoba na javnim mjestima može imati **negativan učinak**

330 Vidi: Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, pripremljen za the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) Vijeća Europe, 2015, odlomak I.iii, *The dangers inherent in data mining and profiling*, dostupno na: https://rm.coe.int/16806a601b

331 A to je razlog zašto su, posebno restriktivna, pravila o obradi osobnih podataka uključena u europske instrumente zaštite osobnih podataka: vidi "NB" u Prvom dijelu, odlomak 1.2.3, na str. 17, prethodno u tekstu. Vidi: *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes, 16. veljače 2012. g., dostupno na: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnantbefore-her-father-did/#2ea04af16668

332 Vidi: How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, Forbes, 16. veljače 2012.g., dostupno na: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnantbefore-her-father-did/#2ea04af16668

na ostvarenje temeljnih prava, kao što su pravo na slobodu izražavanja, udruživanja i prosvjeda.[333] Štoviše, rizici se mogu kombinirati i potom **međusobno ojačavati jedan drugog**, kao u slučaju korištenja tehnologije prepoznavanja lica kod nadziranja javnih mjesta od strane policije, s ciljem "identificiranja" loših osoba i predviđanja lošeg ponašanja.[334]

Skrećemo pažnju na to da kako bi se ovi rizici doista i pojavili, nije potrebna povreda podataka: rizici proistječu iz inherentno opasnih karakteristika samih postupaka obrade, čak i ako se provode sukladno njihovim specifikacijama i bez povrede podataka kako je definirano u GDPR-

u. ***Ovo nije obuhvaćeno (inače vrlo korisnom) shemom procjene rizika kojeg je iznio* Garante, *što je prikazano ranije u tekstu.***

Isto vrijedi u pogledu manjih "rizika za prava i slobode pojedinaca", koji proizlaze iz postupaka obrade, koji nisu popisani kao rizici koji inherentno predstavljaju "visok rizik". Ovo uključuje posebice postupke obrade koji ne udovoljavaju u cijelosti zahtjevima GDPR-a.

PRIMJERI:

- Korištenje osobnih podataka prikupljenih za neku od svrha, koje nije "kompatibilno" svrsi bez valjane pravne osnove za sekundarnu obradu i/ili bez primjerenog obavještavanja ispitanika o namjeravanim sekundarnim korištenjima njihovih podataka – što bi bilo još gore ako to uključuje otkrivanje podataka trećoj strani.

Ovo može dovesti do toga da se ispitanicima uskrati mogućnost davanja privole (ili uskrate privole ili prigovora) za sekundarnu obradu, što može imati negativne učinke za njih (npr. na poslu i odobravanju kredita). Također je prilično vjerojatno da osobni podaci pribavljeni u jednom kontekstu nisu dostatno točni ili relevantni za korištenje u potpuno različitom kontekstu.

- Zadržavanje i/ili korištenje osobnih podataka (uobičajeno, kad isti više nisu potrebni za izvornu svrhu u koju su prikupljeni) u pseudonimiziranom ili navodno anonimiziranom obliku (tipično, za daljnje korištenje u ovom obliku za novu, sekundarnu svrhu).

U smislu povećanog rizika kod ponovne identifikacije čak i navodno potpuno anonimiziranih podataka[335], bilo koje takvo zadržavanje i korištenje pseudonimiziranih ili navodno anonimiziranih podataka mora se smatrati kao da predstavlja rizike za prava i slobode ispitanika (što čak može postati "visoki rizici", koji zahtijevaju procjenu učinka na zaštitu podataka, kao što se opisuje u 4. zadaći). SZP bi iznimno pažljivo trebao provjeriti rizike ponovne identifikacije takvih podataka kod bilo kojih specifičnih korištenja, i nametnuti snažne ublažavajuće faktore (kao što je "diferencijalna privatnost")[336] u odgovarajućim slučajevima – ili odbiti dopustiti daljnju obradu podataka.

- Korištenje nebitnih, netočnih ili zastarjelih informacija – s mogućim sličnim negativnim posljedicama.

333 Vidi citat iz poznate presude *Census* judgment njemačkog Ustavnog suda na str. 10 ovog priručnika. [338] Vidi: Douwe Korff, *First Do No Harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions*, odlomak 2.4, *Preventive, predictive policing*, u: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (Eds.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Centre for Internet and Human Rights, Berlin, na redu za objavu kasnije tijekom 2018.

334 Vidi: Douwe Korff, First Do No Harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions, odlomak 2.4, Preventive, predictive policing, u: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (Eds.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Centre for Internet and Human Rights, Berlin, na redu za objavu kasnije tijekom 2018.

335 Za lako čitljiv sažetak pitanja oko ponovne identifikacije, vidjeti podnesak Zaklade za istraživanje informacijske politike (the Foundation for Information Policy Research) to the UK Government consultation on Making Open Data Real, listopad 2011., dostupno na: www.fipr.org/111027opendata.pdf. Ovo se odnosi na poticajan rad o tom problemu: Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, 57 UCLA Law Review (2010) 1701, dostupno na: http://papers.ssrn.com/sol3/papersfm?abstract_id=1450006.

336 Diferencijalna privatnost je važna mjera za sprječavanje ponovne identifikacije ispitanika iz nizova podataka – ali to radi samo ako se primijeni u kontroliranoj okolini, u kojoj su istraživači ograničeni na upite koje mogu slati bazi podataka, vidi: https://privacytools.seas.harvard.edu/differential-privacy https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf Ne pruža odgovor kod okolnosti u kojima su osobni podaci pušteni u navodno potpuno anonimiziranom obliku široj javnosti, ili pak u kojima veliki nizovi podataka su drugačije upareni bez potpune kontrole.

- Nepridavanje odgovarajuće težine "ispitanikovim interesima ili temeljnim pravima i slobodama koje zahtijevaju zaštitu osobnih podataka, posebice kada je ispitanik dijete", kod procjene mogu li se osobni podaci obrađivati po osnovi uvjeta "legitimnih interesa" (čl. 6(1)(f) GDPR).

Ovo po definiciji izaziva štetu za te interese ispitanika. Korištenje kriterija "legitimnog interesa" kao pravne osnove za obradu stoga uvijek zahtijeva posebno pomno propitivanje od strane SZP-a u ovoj zadaći.

NB: Na kriterij se ne mogu osloniti javna tijela "pri izvršavanju svojih zadaća" (čl. 6(1), posljednja rečenica), ali to ne znači da se pitanje nikada ne javlja u kontekstu javnog sektora, npr. u odnosu na zadaće koje nisu propisane zakonom, kao što je slanje e-pošte građanima o kulturnim događanjima, korištenje popisa stanovništva; ili u vezi s aktivnostima pravnih osoba koje provode zadaće "u javnom interesu".

- Nepravilno pružanje informacija ispitaniku o svim detaljima kojih je mnogo, o kojima moraju biti obaviješteni po osnovi članka 13. i 14. Uredbe.

Ovo može dovesti do toga da ispitanici nisu u mogućnosti u cijelosti ostvariti svoja prava temeljem Uredbe (što su naravno upravo oblici "interes[a] ili temeljna[ih] prava i slobode[a] ispitanika koji zahtijevaju zaštitu osobnih podataka").

- Prijenos osobnih podataka u treću zemlju za koju se smatra da ne pruža "primjerenu" zaštitu osobnim podacima, bez postojanja odgovarajućih zaštitnih mjera ili setova odobrenih obvezujućih korporativnih pravila (OKP-ovi), ili bez na drugi način oslanjanja na jedno od specificiranih izuzeća (usp. članak 46 – 48 GDPR-a). Ovo uključuje korištenje usluge u oblaku ("cloud") koja koristi poslužitelj (ili poslužitelje) koji se nalaze u takvim trećim zemljama.

Kako je istaknuo ENZP u svojem detaljnom savjetu o korištenju usluga u oblaku ("cloud") od strane EU institucija (što bi također trebala proučiti nacionalna javna tijela jer bi se velik dio tog savjeta mogao jednako primijeniti i na njih), računarstvo u oblaku predstavlja specifične rizike kojima bi voditelji obrade trebali pristupiti iznimno pažljivo (oslanjajući se na svoje SZP-e).[337] Doista, njegov savjet sugerira da se za računarstvo u oblaku može itekako smatrati da inherentno predstavlja visoke rizike i stoga traži procjenu učinka na zaštitu podataka. Ovo se spominje u sljedećoj zadaći.

- Izdvajanje poslova obrade osobnih podataka vanjskim suradnicima (outsourcing) od strane javnih tijela, posebice ako su podaci osjetljivi u tehničko-pravnom smislu iz Uredbe ("posebne kategorije podataka" – članak 9), ili osjetljivi podaci u općenitijem smislu, kao što su financijski podaci ili podaci o popisu stanovništva.

ENZP primjećuje da korištenje računarstva u oblaku ojačava rizike inherentne kod outsourcinga usluga obrade.[338]

Ako, nakon što je provedena procjena učinka na zaštitu podataka, prema mišljenju SZP-a, postupci obrade osobnih podataka predstavljaju rizik za relevantne interese, SZP mora **dati savjet** relevantnoj interno odgovornoj osobi ili osobama o tim rizicima, te predložiti **ublažavanje rizika ili alternativni postupak**. Često, legitimna svrha se može postići različitim, manje ometajućim načinima, ili korištenjem manje (i manje osjetljivih) podataka – a u takvim slučajevima, SZP bi trebao snažno sugerirati da u slučaju ako se ovaj savjet ne slijedi, SZP ponovo treba **uputiti** ovo pitanje najvišim upravljačkim strukturama (vidi dalje pod "*Savjetodavne zadaće*").

Opet, SZP bi trebao voditi cjelovite **evidencije** o svim ovim procjenama rizika i savjetima.

337 European Data Protection Supervisor (EDPS), Guidelines on the use of cloud computing services by the European institutions and bodies, ožujak 2018, dostupno na: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf Posebno vidjeti Prilog 4: Data protection-specific risks of cloud computing

338 The EDPS Guidelines on the use of cloud computing services by the European institutions and bodies (prethodna bilješka) „fokusira se na korištenje usluga računarstva u oblaku koje pružaju komercijalne kompanije [ali] kao takav također se, kao prirodnom posljedicom, bavi pitanjima koja se javljaju radi tzv. outsourcinga (angažiranja vanjskih pružatelja usluga) IT usluga koji obrađuju osobne podatke". (str. 5).

Ako se savjet SZP-a ostvari, ove evidencije će "**dokazati** da se obrada provodi u skladu s ovom Uredbom" – tj., da su ovi rizici doista bili procijenjeni i da su mjere poduzete u svjetlu te procjene bile prikladne tim rizicima (usp. čl. 24(1) i raspravu o "obvezi dokazivanja sukladnosti" s Uredbom pod točkom 2.2, ranije u tekstu).

Napominjemo da ako opća procjena rizika ukazuje da predložena obrada predstavlja mogući "**visok rizik**" za prava i slobode pojedinaca, SZP treba savjetovati voditelja obrade da je potrebna cjelovita procjena učinka na zaštitu podataka (PUZP), kako se u nastavku opisuje, u 4. zadaći.

Primijetite da, čak i ako PUZP nije potreban, SZP će morati nastaviti pratiti sve svoje postupke obrade osobnih podataka na kontinuiranoj osnovi: vidi raspravu nakon 4. zadaće, pod naslovom "*Praćenje sukladnosti: Kontinuirano ponavljanje zadaća 1 – 3 (i 4)*".

Također zamijetite da su se često nacionalni zakonodavci već pokušali pozabaviti posebnim rizicima za koje vjeruju da su nastali posebnim postupcima obrade ili radnjama, u svojim nacionalnim pravilima – nešto što se u velikoj mjeri može nastaviti pod posebnim klauzulama u Uredbi **Primjeri:**

U **Hrvatskoj**, obrada ***genetskih podataka*** za izračun rizika od obolijevanja i drugih zdravstvenih aspekata ispitanika u odnosu na sklapanje ili izvršenje ugovora o životnom osiguranju i ugovorima s klauzulama o doživljenju je zabranjena – i ova se zabrana ne može ukloniti privolom ispitanika (članak 20. Zakona o provedbi Opće uredbe o zaštiti podataka).

U Hrvatskoj, a i u drugim državama, korištenje ***biometrijskih podataka*** i ***videonadzornog sustava (CCTV)*** također podliježe posebnim uvjetima, kao što je zahtjev za posebno jasnom i nedvosmislenom privolom, te ograničenja, kao što je vremensko ograničavanje zadržavanja podataka.

Takvi zakonski uvjeti bi također trebali biti u cijelosti uzeti u obzir kod bilo koje procjene rizika: ni jedan voditelj obrade ili SZP ne bi naravno nikada zaključio da je rizik prihvatljiv iako nije udovoljeno posebnim zakonskim uvjetima i ograničenjima.

4. ZADAĆA *Rješavanje postupaka obrade koji predstavljaju mogućnost "visokog rizika": provođenje procjene učinka na zaštitu podataka (PUZP)*

Što je gore navedeno o općoj procjeni rizika (3. zadaća) primjenjuje se *a fortiori* na postupak obrade osobnih podataka koji se, na osnovi gornje opće procjene rizika, smatra da predstavlja "**visok rizik** za prava i slobode pojedinaca" (čl. 35(1)). Uredba jasno propisuje da ovo posebno može biti slučaj kada se koriste "nove tehnologije".

Ako preliminarna procjena rizika provedena u 3. zadaći doista ne ukazuje na to da određeni postupak obrade osobnih podataka predstavlja takav "visoki rizik", tada se od voditelja obrade traži da provede **procjenu učinka na zaštitu podataka** (PUZP) prije nastavka postupka.

Uredba propisuje da se PUZP u svakom slučaju mora provesti u slučajevima da se u cijelosti primjenjuje automatizirano donošenje odluka, uključujući izradu profila, opsežnu obradu osjetljivih podataka, ili opsežno praćenje javno dostupnih područja (članak 35(3)). Nacionalna nadzorna tijela također moraju usvojiti popise postupaka koji će biti podvrgnuti PUZP-u na njihovom teritoriju, te mogu usvojiti popise postupaka koje neće trebati isto – ali ovi popisi moraju biti predani EOZP-u, a mogu ih osporiti druga nadzorna tijela sukladno "mehanizmu konzistentnosti" Uredbe (članak 35(4) – (6)). Uredba također dopušta EOZP-u da izda obje vrste popisa postupaka, nastavljajući na popisima koje su mu predala nacionalna nadzorna tijela (od kojih se traži da to učine temeljem članka 64(1)(a) Uredbe).

U praksi, dogodilo se to da je, prije svega, Radna skupina iz članka 29. izdala opsežan savjet i smjernice o

provođenju PUZP-a, i u svojim Smjernicama o SZP-ovima iz prosinca 2016. g., u revidiranom obliku iz travnja 2017. (RS243 rev1)[339] i u svojim kasnijim, opširnijim Smjernicama o PUZP-ima, usvojenima 4. travnja 2017. g., koje su revidirane i usvojene 4. listopada 2017. g. tj., sve i dalje prije primjene Uredbe).[340] Obje je podržao Europski odbor za zaštitu podataka na dan kada je Uredba u cijelosti stupila na snagu, 25. svibnja 2018. g.[341] ENZP (Europski nadzornik za zaštitu podataka) je također pružio daljnje korisne smjernice u svojem radu na temu Accountability on the ground (Pouzdanost [odgovornost] u praksi)[342] uključujući privremeni popis postupaka obrade koji, po njegovom mišljenju, zahtijevaju ili ne zahtijevaju provođenje PUZP-a.[343]

Revidirane Smjernice o PUZP-ima, koje je usvojio RS29 i podržao EOZP, navode **devet kriterija** koje treba uzeti u obzir kod određivanja predstavlja li postupak obrade "visok rizik", i kažu da:[344]

> ***U većini slučajeva***, voditelj obrade može smatrati da bi obrada koja ispunjava **dva kriterija** zahtijevala provedbu PUZP-a. Općenito, RS29 smatra da što je više kriterija zadovoljeno nekom obradom, to je vjerojatnije da predstavlja visok rizik za prava i slobode ispitanika, te stoga zahtijeva PUZP, neovisno o mjerama koje je voditelj obrade zamislio usvojiti.

O ovome se dalje raspravlja u nastavku, pod naslovom "*kako procijeniti predstavlja li predloženi postupak obrade visoke rizike*", gdje su izneseni primjeri uzeti iz Smjernica RS29 i rada Europskog nadzornika za zaštitu podataka, pod podnaslovom "Čimbenici koji ukazuju na visoke rizike".

Ovdje bismo naglasili da je, potom, većina nadzornih tijela (22 od 28)[345] usvojila svoje vlastite privremene popise i predala ih Europskom odboru za zaštitu podataka na pregled. EOZP je proveo te provjere u svjetlu Smjernica RS29 koje je podržao, te je na dan 25. rujna 2018. godine izdao 22 mišljenja o tim popisima (jedan o svakom nacrtu popisa).[346] Glavni naglasak koji Europski odbor za zaštitu podataka kontinuirano stavlja u tim mišljenjima bio je preporuka nadzornim tijelima da ne bi trebali uključivati postupke obrade u popis postupaka za koje je PUZP obvezan, ako je dotični postupak udovoljio samo *jednom* od kriterija za određivanje postojanja "visokog rizika", navedenog u Smjernicama. Stoga, primjerice, prema njihovom mišljenju o nacrtu popisa kojeg je predalo Ujedinjeno Kraljevstvo, kaže se:[347]

> Popis kojeg je Odboru predalo nadzorno tijelo Ujedinjenog Kraljevstva na mišljenje navodi da obrada biometrijskih podataka sama po sebi spada pod obvezu provođenja PUZP-a. Odbor je mišljenja da obrada biometrijskih podataka sama po sebi ne mora nužno predstavljati visok rizik. Međutim, obrada biometrijskih podataka u svrhe jedinstvenog identificiranja pojedinca u sprezi s najmanje još jednim drugim kriterijem zahtijeva provedbu PUZP-a. Stoga Odbor zahtijeva od nadzornog tijela Ujedinjenog Kraljevstva da na odgovarajući način izmijeni svoj popis, dodajući da stavka koja navodi da obrada biometrijskih podataka u svrhe jedinstvenog identificiranja fizičke osobe zahtijeva provedbu PUZP-a samo kada se to čini u sprezi s najmanje još jednim kriterijem, bude primijenjena ne dovodeći u pitanje članak 35(3)Uredbe.

---

339 Vidi bilješku 242, prethodno

340 RS29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (RS248 rev 1, dalje u tekstu označene kao RS29 Smjernice o PUZP-ima), stranica sadržaja, dostupno na: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

341 Vidi bilješku 248, prethodno.

342 EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (bilješka 302, iznad), odlomak 4, *When to carry out a DPIA?*, na str. 9-11.

343 Idem, Prilog 5.

344 RS29 Smjernice o PUZP-ima (bilješka 351, iznad), str. 11, dodan naglasak.

345 Austrija, Belgija, Bugarska, Češka Republika, Njemačka, Estonija, Grčka, Finska, Francuska, Mađarska, Irska, Italija, Litva, Latvija, Malta, Nizozemska, Poljska, Portugal, Rumunjska, Švedska, Slovačka i Ujedinjeno Kraljevstvo.

346 Sve je dostupno putem poveznica dostupnih na: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

347 EOZP, Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject to the requirement of a data protection impact assessment (članak 35.4 GDPR), adopted on 25 September 2018, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25opinion_2018_art._64_uk_sas_dpia_list_en.pdf

Ali, naravno, voditelj obrade može provesti PUZP čak i ako je udovoljeno samo jednom od tih kriterija, bez da je to obveza.

Zahtjev za provedbom PUZP-a može se otkloniti u slučajevima kada zakon regulira vrstu odgovarajućeg postupka, a opći PUZP je proveden u kontekstu donošenja zakona (članak 35(10)). Nadalje, "[a] jedna [PUZP] procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike" (članak 35(1), posljednja rečenica). Kako je RS29 zaključio:[348]

> Kada PUZP nije potreban? Kada nije "vjerojatno da će [obrada] prouzročiti visok rizik", ili postoji sličan PUZP, ili je bila odobrena prije svibnja 2018. g., ili ima pravnu osnovu, ili je na popisu postupaka obrade za koje se PUZP ne traži.

Opširne smjernice o PUZP-ima, uključujući metodološke smjernice, također su izdala i nacionalna tijela za zaštitu podataka, uključujući ona u Francuskoj, Španjolskoj i UK-u, kao i od strane njemačkog *Datenschutz-zentrum* (kojeg podržavaju njemačka nadzorna tijela).[349] **Francusko** je tijelo za zaštitu podataka, CNIL, čak (u suradnji s ostalim nadzornim tijelima) razvilo softverski alat otvorenog koda za PUZP koji "ima za cilj pomoći voditeljima obrade da izgrade i dokažu sukladnost s Uredbom". Kako se objašnjava na mrežnim stranicama:[350]

Tko može koristiti softver za PUZP?

Alat je uglavnom namijenjen voditeljima obrade koji su pomalo upoznati s procesom PUZP-a. U tom smislu, samostalna se verzija može preuzeti (*download*) i lako pokrenuti na Vašem računalu.

Također je moguće koristiti alat na poslužiteljima organizacije kako bi se isti integrirao s drugim alatima i sustavima koji se već koriste unutar organizacije.

Što je to?

PUZP alat je dizajniran na osnovi tri načela:

- **Didaktičko sučelje za provedbu PUZP procjena:** alat se oslanja na sučelju prilagođeno korisniku kako bi se omogućilo jednostavno upravljanje Vašim PUZP-ima. Ono jasno otkriva metodologiju procjene učinka na zaštitu podataka korak po korak. Nekoliko vizualizacijskih alata nudi načine za brzo uviđanje rizika.
- **Pravna i tehnička baza znanja:** alat uključuje pravne točke osiguravajući zakonitost obrade i prava ispitanika. Također ima i kontekstualnu bazu znanja, koja je dostupna slijedom svih koraka PUZP-a, prilagođavajući prikazani sadržaj. Podaci su izvučeni iz Uredbe, PUZP vodiča i CNIL-ovog Sigurnosnog vodiča/Security Guide, prema aspektu obrade koji se proučava.
- **Modularni alat:** dizajniran kako bi Vam pomogao u građenju svoje sukladnosti, možete prilagođavati alat sadržaja prema svojim specifičnim potrebama ili poslovnom sektoru, primjerice kreiranjem PUZP modela kojeg možete duplicirati i koristiti za niz sličnih postupaka obrade. Objavljen pod besplatnom licencom, moguće je modificirati izvorni kod alata kako bi se dodala svojstva ili kako bi ga se uključilo u alate koje koristi Vaša organizacija.

348 RS29 Smjernice o PUZP-ima (bilješka 315, prethodno u tekstu), stranica sadržaja, str. 6.

349 Vidi popis s poveznicama u *Prilogu 1* uz RS29 Smjernice o PUZP-ima (bilješka 315, prethodno u tekstu). Metodologije za PUZP se obrazlažu dalje u tekstu, pod tim naslovom.

350 Dostupno, s daljnjim informacijama na engleskom, na: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment CNIL koristi kraći akronim "PIA" (također u citiranom tekstu, iznad), vjerojatno jer PUZP ima podrijetlo u "*Privacy* Impact Assessments". Primijetite da je alat nedavno ažuriran. Informacije o ažuriranju su dostupne ovdje (samo na francuskom): https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd
Na toj stranici, CNIL kaže da je softver dostupan na 14 jezika: francuski, engleski, talijanski, njemački, poljski, mađarski, finski, norveški, španjolski, češki, nizozemski, portugalski, rumunjski i grčki, te da ga podržavaju (barem privremeno, u beta verziji) tijela za zaštitu podataka iz Bavarske, Italije, Finske, Mađarske, Poljske i Norveške. Međutim, primijetite da se softver uglavnom fokusira na tehničku sigurnost, te će ga uglavnom koristiti MSP-ovi, a ne velike i vrlo složene pravne osobe.

U ovom priručniku nema dovoljno prostora za iznošenje svih detaljnih savjeta o PUZP-ima koji su izneseni u kasnijim, podrobnijim smjernicama RS29 o PUZP-ima (podržanima od Europskog odbora za zaštitu podataka), ili u nacionalnim smjernicama: čitatelja se snažno potiče da prouči smjernice **RS29/Europskog odbora za zaštitu podataka u cijelosti, kao i relevantne nacionalne savjete kada je to relevantno, te da se oslanja na iste u svojim radnjama i da se oslanja na bilo koje dobivene savjete.**[351]

Čitatelj, a posebice SZP-ovi, bi također trebali uzeti u obzir nacionale obvezne PUZP popise koje je objavilo njihovo nadzorno tijelo jer taj popis sadrži primjere situacija gdje je primjena gornjih smjernica i savjeta dovela do propisivanja provedbe PUZP-a i za javne i za privatne pravne osobe; od SZP-ova se očekuje da nadziru provođenje PUZP-a od strane odnosnih voditelja obrade kada god im je određeno da to čine temeljem spomenutih popisa. Ako se također izdaju i "bijeli popisi" u sljedećih nekoliko mjeseci (sukladno članku 35(5) GDPR-a), i oni će također biti prilično korisni jer će se njima isključiti potreba da voditelj obrade provede ovu praksu za niz postupaka obrade koji nisu visokog rizika.

U nastavku ćemo kratko navesti smjernice vezano za: **različite uloge i odgovornosti voditelja obrade i SZP-a**; pitanje **kako procijeniti predstavlja li predloženi postupak obrade "visok rizik"**; **metodologije za PUZP-ove**, i što učiniti s evidencijom **PUZP-a**, posebice ako je zaključeno da se određeni identificirani visoki rizici ne mogu u cijelosti ublažiti različitim mjerama, u kojem slučaju Uredba zahtijeva da **se konzultira nadležno tijelo nadzorno tijelo** (čl. 36).

RAZLIČITE ULOGE I ODGOVORNOSTI VODITELJA OBRADE I SZP-A U ODNOSU NA PUZP

U svojim Smjernicama o SZP-ovima, RS29 je ponovo naglasio različite uloge i odgovornosti voditelja obrade i SZP-a, također u odnosu na PUZP. Tekst glasi:[352]

> 4.2. Uloga SZP-a u procjeni učinka na zaštitu podataka
>
> Prema članku 35(1), zadaća je voditelja obrade, a ne SZP-a, provesti, kada je to potrebno, procjenu učinka na zaštitu podataka (PUZP). Međutim, SZP može odigrati vrlo važnu i korisnu ulogu pomažući voditelju obrade. Slijedeći načelo cjelovitosti podataka, članak 35(2) izrijekom zahtijeva da voditelj obrade "traži savjet" od SZP-a pri provođenju PUZP-a. Članak 39(1)(c), pak zadužuje SZP obvezom u smislu "*pružanja savjeta, kada je to zatraženo, u pogledu [PUZP] i praćenje njegova izvršavanja*".
>
> RS29 preporučuje da bi voditelj obrade trebao zatražiti savjet od SZP-a, o sljedećim pitanjima, između ostaloga:[353]
>
> - treba li ili ne provesti PUZP;
> - koju metodologiju slijediti kod provođenja PUZP-a;
> - treba li PUZP provesti unutar kuće ili je povjeriti vanjskom pružatelju usluga;
> - koje zaštitne mjere (uključujući organizacijske i tehničke mjere) primijeniti da bi se ublažili rizici za prava i interese ispitanika;
> - je li ili nije PUZP bio ispravno proveden i jesu li njegovi zaključci (o tome treba li nastaviti ili ne s obradom i koje zaštitne mjere primijeniti) sukladni s GDPR-om.
>
> Ako se voditelj obrade ne slaže sa savjetom kojeg je dao SZP, dokumentacija o

351 Vidi reference u bilješkama 249, 318, 351 i 353 i u prethodnoj bilješci, iznad, za glavni savjet koji treba proučiti.
352 RS29 Smjernice o SZP-ima(bilješka 242, prethodno u tekstu), odlomak 4.2, str. 16-17, izvornik u kurzivu, podvlačenje u posljednjem stavku dodano.
353 Članak 39(1) spominje zadaće SZP-a i navodi da će SZP imati "barem" sljedeće zadaće. Stoga, ništa ne priječi voditelja obrade da dodijeli SZP-u druge zadaće osim onih spomenutih u članku 39(1), ili da specificira te zadaće detaljnije.

PUZP-u treba posebice opravdati u pisanom obliku zbog čega savjet nije uzet u obzir.[354]

RS29 dalje preporučuje da voditelj obrade jasno skicira, primjerice u ugovoru sa SZP-om, ali također i u informacijama koje su pružene zaposlenicima, upravi (i drugim dionicima, kada je to relevantno), precizne zadaće SZP-a i njihov opseg, posebice u pogledu provođenja PUZP-a.

Kasnije RS29 u Smjernicama o PUZP-ima također naglašava da PUZP trebaju provesti "[v]oditelj obrade, sa SZP-om i izvršiteljima obrade".[355]

U praksi, posebno u manjim organizacijama, SZP će često ponovo odigrati jednu od vodećih uloga (ako ne baš i jedinu) u procjeni.

KAKO PROCIJENITI PREDSTAVLJA LI PREDLOŽENI POSTUPAK OBRADE "VISOKI RIZIK"

RS29/EOZP objašnjavaju da:[356]

Obveza za voditelje obrade da provedu PUZP u određenim okolnostima trebala bi se shvatiti kao pozadina njihove opće obveze na odgovarajući način upravljati rizicima koji se javljaju uslijed obrade osobnih podataka.

Drugim riječima, kako je također objašnjeno ranije, pitanje o tome treba li procjena učinkabiti provedena javlja se prirodno iz opće obveze voditelja obrade – provedena uz "savjet", ali u praksi oslanjajući se na, osobu SZP-a – da procijeni rizike inherentne svim postupcima obrade osobnih podataka voditelja obrade (3. zadaća, prethodno).

Nadalje se razjašnjava koncept "rizika" i zaštićenih interesa koji trebaju biti uzeti u obzir:[357]

"Rizik" je scenarij koji opisuje događaj i njegove posljedice, procijenjene u smislu težine i vjerojatnosti. "Upravljanje rizikom", s druge strane, može se definirati kao koordinirane aktivnosti da se usmjeri i kontrolira organizacija u smislu rizika.

Članak 35. odnosi se na vjerojatan visok rizik "za prava i slobode pojedinaca". Kako je navedeno u Izjavi Radne skupine članka 29. o ulozi pristupa temeljenog na riziku u pravnim okvirima zaštite podataka, pozivanje na "prava i slobode" ispitanika prvenstveno se tiče prava na zaštitu osobnih podataka i privatnosti, ali može također uključivati druga temeljna prava, kao što su sloboda govora, sloboda misli, zabrana diskriminacije, pravo na slobodu mišljenja, savjesti i vjeroispovijesti.

RS29 navodi primjere uz članak 35(3) GDPR-a o situacijama koje inherentno predstavljaju "visoke rizike", već prethodno spomenuto: kada voditelj obrade koristi automatizirane algoritme uz izradu profila za donošenje odluka s pravnim ili drugim značajnim učinkom; kada voditelj obrade posjeduje podatke posebne kategorije ili podatke o kaznenim osudama: "u velikoj mjeri"; ili kada voditelj obrade "sustavno prati" javno dostupna mjesta "u velikoj mjeri". S pravom dodaje:[358]

354 Članak 24(1) propisuje da 'Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju'.

355 Vidi RS29 Smjernice o PUZP-ima (bilješka 351, prethodno u tekstu), odlomak III.D.b).

356 Idem, str. 6.

357 Idem. Primijetite također referencu ranije na ISO 31000:2009, Risk management – Principles and guidelines, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO) (WP29 Smjernice o DPIA-ma, bilješka 351, na str. 5).

358 *Idem*, str. 9.

Kako riječ "osobito" u uvodnoj rečenici članka 35(3) GDPR-a ukazuje, ovo je zamišljeno kao neisključiv popis. Mogu postojati postupci obrade "visokog rizika" koji nisu obuhvaćeni popisom, ali ipak predstavljaju usporedivo visoke rizike. Ti postupci obrade trebaju također biti podvrgnuti PUZP-ima.

RS29 navodi niz čimbenika – većinom, iako ne potpuno, vezanih za tri primjera iz članka 35 – koji ukazuju na to da postupak predstavlja "visoke rizike", i navodi dalje, specifične primjere. ENZP pruža dalje primjere, i u svojem privremenom popisu postupaka obrade koji će uvijek zahtijevati provedbu PUZP-a, a i u predlošku koji se može koristiti za procjenu jesu li postupci obrade koji nisu navedeni ni u njegovom "pozitivnom" popisu (postupci koji će po njegovom mišljenju uvijek zahtijevati PUZP) ni u njegovom "negativnom" popisu (oni koji prema njemu ne zahtijevaju PUZP) trebaju biti podvrgnuti PUZP-u.[359] Ovi primjeri RS29 i ENZP-a navedeni su niže (ponešto uređeni, s primjerima RS29 uklonjenima iz teksta i prebačenima u okvir, dok su primjeri ENZP-a označeni asteriskom*). Mi smo dodali još neke primjere (ili dodatne detalje ili varijacije) koji su posebice relevantni za voditelje obrade iz javnog sektora; ti su primjeri označeni kurzivom (*italic)*.

Čimbenici koji ukazuju na "visoke rizike"[360]

1. Procjena ili bodovanje, uključujući profiliranje i predviđanje, posebno "*analizu i predviđanje aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja*" (uvodne odredbe 71 i 91).

Primjeri:

Financijska institucija koja provjerava svoje klijente preko baze podataka kreditnih referenci ili bazama podataka o sprečavanju pranja novca i borbi protiv financiranja terorizma (AML/CTF) ili prijevare.

Banka koja provjerava transakcije sukladno važećem zakonu radi otkrivanja mogućih prijevarnih transakcija.*

Profiliranje zaposlenika temeljem svih njihovih transakcija u sustavu upravljanja predmetima [dotične organizacije] s automatskom preraspodjelom zadataka.*

Biotehnološka kompanija koja nudi genetičke testove izravno potrošačima kako bi procijenila i predvidjela rizike za razvoj bolesti/zdravstvene rizike.

Trgovačko društvo koje izrađuje bihevioralne ili marketinške profile temeljem korištenja ili navigacije po njihovim mrežnim stranicama.

2. Automatizirano donošenje odluka s pravnim ili sličnim značajnim učinkom: obrada koja smjera na donošenje odluka o ispitanicima koje proizvode "pravne učinke koji se odnose na pojedinca" ili koje "na sličan način značajno utječu na pojedinca" (članak 35(3)(a)), posebice (ali ne isključivo) u slučajevima u kojima obrada može dovesti do isključenja ili diskriminacije na štetu pojedinaca.

Primjeri:[361]

Automatizirano ocjenjivanje zaposlenika ("ako se nalazite među 10% tima po broju najmanje riješenih slučajeva, dobit ćete ocjenu "nije zadovoljio/la" u Vašoj ocjeni radnog učinka, bez rasprave").*

359 Pozitivni i negativni popisi su navedeni u *Prilogu 5* uz EDPS Accountability on the ground paper (bilješka 353, iznad); the *Template for threshold assessment/criteria* je sadržan u *Prilogu 6* tog rada.

360 Kako je popisano i numerirano u RS29 Smjernicama o PUZP-ima (bilješka 351, iznad), str. 9-10. Glavni komentari u odnosu na čimbenike su također uzeti iz tih smjernica. Naglašavamo da se čimbenici ponešto preklapaju, ili se mogu kombinirati, kako je primijećeno pod čimbenicima pod naslovom "*Visokorizične obrade koje uključuju više čimbenika*".

361 RS29/EOZP dodaje da „Obrada s malo učinka ili bez učinka na pojedince ne odgovara ovom specifičnom kriteriju. Daljnja pojašnjenja o tim pojmovima bit će sadržana u skorim RS Smjernicama o profiliranju." (str. 9).

Identifikacija "mogućih" ili "vjerojatnih" poreznih prijevara pomoću automatskog pripisivanja profila poreznim obveznicima. [362]

Identifikacija "mogućih" ili "vjerojatnih" prijevara vezano za socijalna prava temeljem profila poznatih prevaranata.

Identifikacija djece koja su "rizična" kroz odrastanje da postanu pretila ili članovi bande ili kriminalci, ili djevojaka koje će "vjerojatno" ostati trudne u tinejdžerskoj dobi, na temelju profila.[363]

Identifikacija mladih osoba i odraslih kao "rizičnih" da postanu "radikalni".

3. Sustavno praćenje: postupak koji se koristi za promatranje, praćenje ili kontrolu ispitanika, uključujući podatke prikupljene putem mreža ili "sustavnog praćenja javno dostupnog područja u velikoj mjeri" (članak 35(3)(c)). Ova vrsta praćenja je kriterij jer se osobni podaci mogu prikupiti u okolnostima kada ispitanici moguće nisu svjesni tko prikuplja njihove podatke i kako će se isti koristiti. Osim toga, moglo bi biti nemoguće pojedincima izbjeći biti subjekt takvog praćenja u javnosti (ili na javno dostupnom) mjestu(mjestima).

Primjeri:

Analiza mrežnog prometa koja dešifrira enkripciju.*

Skriveni CCTV.*

Smart CCTV [*npr. korištenje softvera za prepoznavanje lica*] na javno dostupnim mjestima.*

Alat za sprječavanje gubitka podataka koji dešifrira SSL enkripciju.*

Obrada meta-podataka (npr. vrijeme, priroda i trajanje bankovne transakcije) za organizacijske svrhe ili da bi se osigurale proračunske procjene.[364]

4. Osjetljivi podaci ili podaci iznimno osobne prirode: ovo uključuje posebne kategorije osobnih podataka kako su definirani u članku 9. (*osobni podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, zdravstvene, genetske ili biometrijske podatke i podatke o seksualnoj orijentaciji*), kao i osobni podaci koji se odnose na kaznene osude ili kažnjiva djela kako je definirano u članku 10. Izvan ovih odredbi iz GDPR-a, za neke se kategorije podataka može smatrati da povećavaju mogući rizik za prava i slobode pojedinaca. Ti se osobni podaci smatraju osjetljivima (na način kako se ovaj izraz uobičajeno tumači) zbog toga što su povezani uz kućanstvo i privatne aktivnosti (*vidi treći primjer, dalje u tekstu*), ili zato što utječu na ostvarivanje temeljnog prava (*vidi četvrti primjer*) ili zato što njihova povreda očigledno uključuje ozbiljan učinak na svakodnevni život ispitanika (*vidi peti primjer*). U tom smislu, moglo bi biti relevantno jesu li podaci već učinjeni javno dostupnima od strane ispitanika ili trećih strana. Činjenica da su osobni podaci javno dostupni može se smatrati čimbenikom kod procjene, [*uzimajući u obzir je li ispitanik mogao razumno očekivati da bi druge osobe mogle koristiti podatke za određene svrhe: vidi sedmi primjer, niže u tekstu*].

362 Takve atribute je u Italiji napravila talijanska Agencija za prihode, koristeći alat nazvan Redditometro. Profili su se zasnivali, između ostalog, na presumiranim troškovima poreznih obveznika oduzetih, prema statističkim parametrima, od njihovog raspoređivanja u posebne obiteljske kategorije ili geografska područja. Ovaj alat za profiliranje je istražio talijanski TZP, Garante. Jedno od glavnih pitanja je bio niska kvaliteta podatka, što je rezultiralo visokom stopom grešaka na temelju nepouzdanih smetnji izvučenih iz podataka. Na temelju istrage, Garante je propisao da se stvaran prihod poreznih obveznika može računati samo od stvarnih, dokumentiranih troškova, a ne ga deducirati iz statistički utemeljenim pretpostavkama o razinama troškova. Vidi: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110

363 Vidi the UK Foundation for Information Policy (FIPR), Childrens Databases - Safety & Privacy, study for the UK Information Commissioner, 2006, dostupno na: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

364 Ovaj je primjer uzet s talijanskog PUZP popisa kojeg je odobrio EOZP.

Primjeri:

Opća bolnica [ili ured socijalne skrbi] koja čuva zdravstvene kartone pacijenata [ili tražitelja socijalne skrbi].

Privatni istražitelj koji čuva detalje o kaznenim osudama ili kažnjivim djelima, [*ili javno tijelo kao što je državna obrazovna institucija koja čuva takve podatke u odnosu na učenike ili studente u takvim institucijama*].

[*Javno tijelo ili pravna osoba (kao što je poslodavac*)] koje pristupa osobnim ispravama, e-pošti, dnevnicima ili bilješkama e-čitatelja opremljenih svojstvima za bilježenje bilješki, u vlasništvu zaposlenika *[ili koje koristi osoblje i za osobne i profesionalne svrhe, kao u situacijama "Ponesi svoj uređaj"/"Bring Your Own Device" [BYOD*]].

[*Javno tijelo ili pravna osoba (kao što je poslodavac*)] koje pristupa vrlo osobnim informacijama sadržanima u aplikacijama s dnevničkim zapisima */life-logging applications, ili korištenje informacija s društvenih mreža u kontekstima koji imaju značajan učinak na dotičnog pojedinca, kao što je odabir kandidata za posao (ili čak intervjui).*

Medicinski pregledi prije zaposlenja i provjere kaznene evidencije.*

Administrativne istrage i disciplinski postupci.*

Bilo kakvo korištenje 1:n biometrijske identifikacije.*

Fotografije korištene sa softverom za prepoznavanje lica ili korišteno radi zaključivanja o drugim osjetljivim podacima [*npr. kada oni mogu dovesti do diskriminacije u kontekstu postupka odabira kandidata za posao*].*

5. *opsežna obrada podataka:* GDPR ne definira što predstavlja termin "opsežno", premda uvodna odredba 91 pruža neke smjernice.[365] U svakom slučaju, RS29 preporučuje da sljedeći čimbenici, posebice, budu razmotreni kod određivanja je li obrada opsežna:
   a. broj dotičnih ispitanika, bilo kao specifična brojka ili izraženo u smislu omjera relevantne populacije;
   b. količina podataka i/ili niz različitih podataka koji se obrađuju;
   c. trajanje ili stalnost aktivnosti postupka obrade;
   d. zemljopisni opseg aktivnosti obrade.

Primjer:

*[Nacionalne ali moguće povezane s onima u EU] baze podataka o praćenju bolesti.**

Opsežna razmjena podataka između voditelja obrade iz javnog sektora (npr. ministarstva, lokalne i područne samouprave itd.) putem elektroničkih mreža.[366]

Opsežno prikupljanje genealoških informacija o obiteljima osoba koje pripadaju određenoj religijskoj skupini. [367]

365 Relativno objašnjenje u Uvodnoj odredbi 91 navodi: ... *"postupci obrade velikog opsega su postupci obrade kojima se nastoji obraditi znatna količina osobnih podataka na regionalnoj, nacionalnoj ili nadnacionalnoj razini i koji bi mogli utjecati na velik broj ispitanika i koji će vjerojatno dovesti do visokog rizika, primjerice zbog osjetljivosti, u kojima se u skladu s postignutom razinom tehnološkog znanja novom tehnologijom koristi u velikom opsegu…"*

366 Ovaj je primjer uzet iz talijanskog PUZP popisa kojeg je odobrio EOZP.

367 Usp. odluka francuskog TZP-a (CNIL) o geneološkom registru mormona, izdan 2013. i prijavljen ovdje: https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-letat-civil-francais.html

Stvaranje vrlo velikih "baza podataka životnog stila" u marketinške svrhe (ali koje bi se mogle – ili bi mogle – također biti korištene za druge svrhe).

Snimanje od strane političkih stranaka uočenih glasačkih namjera vrlo velikog broja glasača (ili kućanstava) diljem nacije ili države, temeljem anketa po kućanstvima te naknadne analize i korištenja tih podataka. [368]

6. Podudarajući ili kombinirani skupovi podataka, [*posebice ako takve baze*] imaju izvor[e] iz dva ili više postupaka obrade podataka koji su vođeni u različite svrhe i/ili [*se provode*] od strane različitih voditelja obrade na način koji bi premašivao razumna očekivanja ispitanika.

Primjer:

Prikriveno unakrsno provjeravanje zapisa (*logs*) pristupnih kontrola, računalnih zapisa i prijava kod fleksibilnog radnog vremena [od strane poslodavca] da bi se otkrili izostanci.*

Porezni ured uparuje svoje evidencije o povratu poreza s podacima o vlasnicima skupih jahti, kako bi našli osobe koje bi možebitno mogle počiniti utaju poreza.[369]

7. Podaci koji se tiču osjetljivih pojedinaca (uvodna odredba 75): obrada ove vrste podataka je kriterij jer povećana neravnoteža moći između ispitanika i voditelja obrade, što znači da pojedinci možebitno ne mogu jednostavno dati suglasnost ili se usprotiviti obradi svojih podataka ili ostvariti svoja prava. Osjetljivi pojedinci mogu uključivati **djecu** (njih se može smatrati kao da nisu u stanju informirano i potpuno se usprotiviti ili dati pristanak na obradu njihovih podataka), **zaposlenici**, ranjiviji segmenti populacije koji zahtijevaju posebnu zaštitu (**mentalno bolesne osobe, tražitelji azila**, ili **starije osobe**, **pacijenti** itd.), te u mnogim slučajevima kada je moguće identificirati neravnotežu u odnosu između pozicije ispitanika i voditelja obrade podataka.

Primjeri:

Korištenje video nadzora i sustava geolokacije kojima se omogućuje udaljeno praćenje aktivnosti zaposlenika.[370]

U osnovi, bilo koja obrada osobnih podataka na bilo kojoj od gore navedenih kategorija osjetljivih pojedinaca, svakako kao i bilo koja obrada osjetljivih podataka o njima, ili opsežna obrada takvih podataka o tim osobama, trebale bi se smatrati kao inherentno "visoko rizične".

8. Inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja. GDPR jasno navodi (članak 35(1) i uvodne odredbe 89 i 91) da korištenje novih tehnologija, definiranih u "skladu s postignutom razinom tehnološkog znanja" (uvodna odredba 91), može izazvati potrebu za provođenjem PUZP-a. Ovo je zato jer korištenje takve tehnologije može uključivati novouvedene oblike ili vrste prikupljanja podataka i korištenja, moguće nevidljive i s visokim rizikom za prava i slobode pojedinaca. Doista, osobne i društvene posljedice lansiranja nove tehnologije mogu biti nepoznate. PUZP će pomoći

368 Ova je praksa čest i doista tradicionalna u UK, kao što je priznato u Uvodnoj odredbi 56 GDPR-a. Ta uvodna odredba kaže da „može se dopustiti iz razloga javnog interesa, pod uvjetom da se uspostave odgovarajuće zaštitne mjere" (dodan naglasak). Ako ništa drugo, ova potreba procijeniti služi li obrada legitimnom javnom interesu i zahtjevu usvajanja „odgovarajućih zaštitnih mjera" ojačava potrebu za ozbiljnom analizom rizika i procjenom učinka.

369 Ovo je učinjeno prije nekog vremena u Nizozemskoj, pod pretpostavkom da velike jahte tipično kupuju porezni prevaranti. Jedna osoba, koja se osjetila prozvanom, podrugljivo je nazvala svoj brod „Black Money".

370 Ovaj je primjer uzet iz talijanskog PUZP popisa kojeg je odobrio EOZP.

voditelju obrade razumjeti i riješiti takve rizike – a mjere umanjivanja trebale bi omogućiti ispitanicima i široj javnosti vidjeti kako i kada, te za koje svrhe bi se nove tehnologije trebale koristiti, tako da se mogu zaštiti od onih koje mogu ugroziti individualna prava i slobode te dovesti do autoritarne vlade ili masovnog praćenja od strane korporacija (ili onih koje djeluju zajednički).

Napomena: U mnogim takvim slučajevima novih tehnologija ili praksi, TZP-ovi (ili EOZP) mogu izdati, ili su već moguće izdali, mišljenja, smjernice ili preporuke – a SZP-ovi bi trebali paziti i provjeravati takve nove dokumente. Ako vjeruju da relevantne smjernice itd. još nisu izdane, trebali bi to provjeriti sa svojim TZP-om. Vidi također 4., 8. i 10. zadaću, dalje u tekstu.

Primjeri:

Kombiniranje korištenja otiska prsta i prepoznavanja lica za poboljšanu kontrolu fizičkog pristupa. [371]

Nove tehnologije namijenjene praćenju radnog vremena i prisustva zaposlenika, uključujući one koje obrađuju biometrijske podatke, kao i druge, kao što je praćenje mobilnih uređaja.[372]

Obrada podataka generiranih korištenjem tzv. aplikacija "Internet stvari" (*povezani, "smart" uređaji i stvari*) ako korištenje podataka ima (ili može imati) značajan učinak na svakodnevni život i privatnost pojedinaca.

Strojno učenje.*

Povezani automobili.*

Praćenje objava prijavljenih kandidata na društvenim medijima.*

9. Kada obrada sama po sebi "*sprječava ispitanike u ostvarenju nekog prava ili korištenju usluge ili ugovora*" (članak 22 i uvodna odredba 91). Ovo uključuje postupke obrade koji imaju za cilj dopuštanje, modificiranje ili odbijanje pristupa ili sklapanja ugovora ispitaniku.

Primjeri:

Banka provjerava svoje klijente putem baze podataka korisnika kredita kako bi odlučila hoće li im ponuditi kredit.

Financijska institucija ili agencija za kreditne reference uzima u obzir dobnu razliku između supružnika da bi odredila kreditnu sposobnost (što može narušiti slobodno ostvarivanje temeljnog prava na brak – i stoga je zabranjeno u Francuskoj od strane francuskog TZP-a, CNIL-a (koje je moralo procijeniti sustav zbog toga što je, s obzirom da su odluke donošene na temelju profila, bio podvrgnut "prethodnom odobrenju" od strane CNIL-a).

Baze podataka o isključenjima.*

Kreditna analiza.*

371 RS29 i nekoliko nacionalnih TZP-ova su izdali detaljne savjete o tome tražeći, između ostalog, da se biološki podaci pohrane na mikroprocesorski čip u uređaju ispitanika, a ne da ih pohranjuje voditelj obrade centralno. Vidi: WP29 Working document on biometrics (RS80, usvojeno 1. kolovoza 2003), str. 6, dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

372 Vidi RS29 Opinion 2/2017 on data processing at work (RS249, usvojeno 8. lipnja 2017), odlomak 5.5, Processing operations relating to time and attendance, na str. 18-19, dostupno na:www.ec.europa.eu/newsroom/document.cfm?doc_id=45631

Visokorizične obrade koje uključuju više kriterija

Kriteriji prethodno navedeni mogu se preklapati ili se kombinirati, npr. "sustavno praćenje" može se preklapati ili biti kombinirano s automatiziranim donošenjem odluka, uključujući izradu profila, te može uključivati opsežnu obradu "osjetljivih podataka". RS29 daje niz primjera obrada s takvim kombiniranim kriterijima) za koje se traži provođenje PUZP-a, kao i primjere obrada kod kojih su prisutni jedan ili više gornjih kriterija), ali kod kojih nije potreban PUZP, kako slijedi:[373]

373 **RS Smjernice o Procjeni učinka za zaštitu osobnih podataka (bilješka 315, iznad), str. 11-12.**

Primjeri obrade	**Mogući relevantni kriteriji**	**Vjerojatnost da se zahtijeva PUZP?**
Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacijski sustav).	- Osjetljivi podaci nadasve osobne prirode. Podaci koji se tiču osjetljivih ispitanika. - Opsežna obrade podataka.	Da
Upotreba sustava kamera radi praćenja vozačkog ponašanja na autocestama. Voditelj obrade zamišlja upotrijebiti sustav pametne video analize za izdvajanje automobila i automatsko prepoznavanje registarskih tablica da bi izdvojio automobile i automatski prepoznao registracijske pločice.	- Sustavno praćenje. - Inovativno korištenje ili primjena tehnoloških ili organizacijskih rješenja.	
Trgovačko društvo sustavno nadzire aktivnosti svojih zaposlenika, uključujući praćenje radnih stanica zaposlenika, aktivnosti na mreži itd.	- Sustavno praćenje. - Podaci koji se tiču osjetljivih ispitanika.	
Prikupljanje podataka s javnih društvenih medija za izradu profila.	- Procjena ili bodovanje. - Opsežna obrada podataka Podudarajući ili kombinirani skupovi podataka. - Osjetljivi podaci nadasve osobne prirode:	
Institucija stvara kreditno bodovanje na nacionalnoj razini ili bazu podataka pronevjera.	- Procjena ili bodovanje. - Automatizirano donošenje odluka s pravnim ili sličnim značajnim učinkom. - Sprječavanje ispitanika od ostvarenja nekog prava ili korištenja usluge ili ugovora. - Osjetljivi podaci ili podaci vrlo osobne prirode:	
Pohrana u svrhe arhiviranja pseudonimiziranih osobnih osjetljivih podataka koji se tiču osjetljivih ispitanika istraživačkih projekata ili kliničkih ispitivanja	- Osjetljivi podaci. - Podaci koji se tiču osjetljivih ispitanika. - Sprječava ispitanike od ostvarivanja prava ili korištenja usluge ili ugovora.	
Obrada "osobn[ih] podat[aka] pacijenata ili klijenata pojedinih liječnika, drugih zdravstvenih djelatnika ili odvjetnika" (Uvodne odredbe 91).	- Osjetljivi podaci ili podaci vrlo osobne prirode. - Podaci koji se tiču osjetljivih ispitanika.	Ne
Mrežni (internetski) časopis koristi popis korisničkih adresa radi slanja generičkog dnevnog sažetka svojim pretplatnicima uz njihovu privolu, a što uključuje	- Opsežna obrada podataka.	
jednostavne načine odjave od daljnjeg slanja poruka.		
Mrežne stranice za elektroničku trgovinu prikazuju oglase za starinske (*vintage*) auto-dijelove, što uključuje ograničeno profiliranje na temelju pregledanih ili kupljenih artikala s njihovih vlastitih mrežnih stranica – opet, uz jednostavnu mogućnost odjave.	- Procjena ili bodovanje.	

METODOLOGIJE ZA PUZP:

Ciljevi PUZP-a su:

(i) precizno **identificirati** (visoke) rizike uključene u predložene postupke obrade, uzimajući u obzir prirodu podataka i obrade, opseg, kontekst i svrhe obrade, te izvore rizika – ne samo u uobičajenim okolnostima, već također i u posebnim okolnostima; i u kratko-, srednje- i dugoročnim okvirima;[374]

(ii) radi **procjene** identificiranih (visokih) rizika, posebice njegovog podrijetla, prirode, a naročito, vjerojatnosti i moguće težine rizika;[375]

(iii) identificirati koje **mjere** se mogu poduzeti da se umanje (visoki) rizici koji su odgovarajući u smislu dostupne tehnologije i troškova primjene, te predložiti takve mjere;[376] i

(iv) **zabilježiti** zaključke, procjene i mjere koje su poduzete (ili nisu poduzete, s razlozima za isto), kako bi se mogla "**dokazati sukladnost**" sa zahtjevima GDPR-a po načelu "pouzdanosti" ["odgovornosti"] u odnosu na procijenjenu obradu.[377]

Članak 35(7) GDPR-a propisuje da (evidencija o) PUZP mora sadržavati "najmanje" sljedeće:

(a) sustavan opis zamišljenih postupaka obrade i svrhe obrade, uključujući, kada je to primjenjivo, legitimni interes kojim se vodi voditelj obrade;

(b) procjena nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama;

(c) procjena rizika za prava i slobode ispitanika iz stavka 1; i

(d) mjere zamišljene za suočavanje s rizicima, uključujući zaštitne mjere, sigurnosne mjere i mehanizme da se osigura zaštita osobnih podataka i dokaže sukladnost s Uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih osoba kojih se to tiče.

RS29 naglašava da:[378]

> Svi relevantni zahtjevi izneseni u GDPR-u pružaju širok, generički okvir za dizajn i provedbu PUZP-a. Praktična primjena PUZP-a će ovisiti o zahtjevima navedenima u GDPR-u, koji se može dopuniti detaljnijim praktičnim smjernicama. **Provedba PUZP-a je stoga podesiva. To znači da čak i mali voditelj obrade može dizajnirati i primijeniti PUZP koji je prikladan za njihove postupke obrade.**

Voditelji obrade mogu stoga (uz konzultiranje svojeg SZP-a) odabrati metodologiju za bilo koji PUZP koji moraju provesti koji baš odgovara njima. Mogu se oslanjati na bilo koje iskustvo koje mogu imati s više tehničkih procjena rizika, npr. prema ISO 31000. Međutim, RS29 je ispravno primijetio različite perspektive iz kojih se PUZP treba provesti prema GDPR-u i (u svakom slučaju, uže sigurnosno orijentiranih) procjena koje se temelje na ISO-u:[379]

> PUZP prema GDPR-u je alat za upravljanje rizicima prema pravima ispitanika, i stoga je potrebna njihova [misli se na ispitanike] perspektiva … Za razliku od toga, upravljanje rizikom na drugim poljima (npr. informacijska sigurnost) se fokusira na [rizike za] organizaciju.

RS29 pruža niz primjera zaštite podataka i metodologija procjena učinka koje su pripremili nacionalni TZP-ovi,[380] te "*potiče razvoj PUZP okvira specifičnih za pojedine sektore*". Sam RS29 je izdao PUZP okvir za RFID aplikacije i PUZP obrazac za Smart Grid i Smart Metering Systems.[381]

374 Usp. Uvodna odredba 90.
375 Usp. Uvodna odredba 84 i ISO 31000.
376 Usp. Uvodna odredba 84.
377 Kako kaže RS29: „PUZP je proces izgradnje i dokazivanja sukladnosti." – RS Smjernice o PUZP-ima (bilješka 351, prethodno u tekstu), str. 4. Za još detalja o načelu pouzdanosti (odgovornosti) i s time vezanim obvezama „dokazivanja sukladnosti", vidi 2. dio priručnika.
378 RS Smjernice o PUZP-ima (bilješka 351, iznad), str. 17, dodan naglasak.
379 Idem.
380 Ponovo pogledati popis s poveznicama u Prilogu 1 uz RS Smjernice o PUZP-ima (bilješka 351, iznad).
381 Idem, bilješke 32 i 33.

Za potrebe ovog priručnika, dostatno je izložiti Kriterije za prihvatljivi PUZP, iznesene u smjernicama RS29:[382]

Prilog 2 – Kriteriji za prihvatljivi PUZP

RS29 predlaže sljedeće kriterije koje voditelji obrade mogu koristiti za procjenu je li PUZP, odnosno je li metodologija za provođenje PUZP-a, dostatno opsežna u smislu sukladnosti s GDPR-om:

- **daje se sustavan opis obrade** (članak 35(7)(a))**:**
  - priroda, opseg, kontekst i svrhe obrade se uzimaju u obzir (uvodna odredba 90);
  - osobni podaci, primatelji i rok na koji se podaci pohranjuju i evidentiraju;
  - izlaže se funkcionalan opis postupka obrade;
  - identificirana su sredstva na kojima se nalaze osobni podaci (hardver, softver, mreže, osobe, papir ili kanali za prijenos papira);
  - sukladnost s odobrenim kodeksima ponašanja [*certifikacije i/ili OKP-ovi*][383] se uzima u obzir (članak 35(8));
- **nužnost i proporcionalnost se procjenjuju** (članak 35(7)(b))**:**
  - mjere zamišljene radi sukladnosti s Uredbom su određene (članak 35(7)(d) i uvodna odredba 90), uzimajući u obzir:
  - mjere koje doprinose proporcionalnosti i nužnosti obrade na temelju:
    - posebne, izričite i zakonite svrhe (članak 5(1)(b));
    - zakonitost obrade (članak 6);
    - primjereni, relevantni i ograničeni na ono što je nužno (članak 5(1)(c));
    - ograničeno trajanje pohrane (članak 5(1)(e));
  - mjere koje doprinose pravima ispitanika:
    - informacije koje se daju ispitaniku (članak 12, 13 i 14);
    - pravo na pristup i prenosivost podataka (članak 15 i 20);
    - pravo na ispravak i brisanje (članak 16, 17 i 19);
    - pravo na prigovor i ograničenje obrade (članak 18, 19 i 21);
    - odnosi s izvršiteljima obrade (članak 28);
    - zaštitne mjere kod međunarodnih prijenosa podataka (Poglavlje V);
    - prethodno savjetovanje (članak 36).
- **rizicima za prava i slobode ispitanika se upravlja (članak 35(7)(c)):**
  - procjenjuju se izvor, priroda, osobitost i ozbiljnost tog rizika (usp. Uvodnu odredbu 84) ili, podrobnije, za svaki rizik (nezakonit pristup, neželjena izmjena i gubitak podataka) iz perspektive ispitanika:
    - uzimaju se u obzir izvori rizika (uvodna odredba 90);
    - identificiraju se potencijalni učinci na prava i slobode ispitanika u slučaju događaja koji uključuju nezakonit pristup, neželjenu izmjenu i gubitak podataka;

382 Idem, Prilog 2. Naglasak podebljanim slovima u glavnim natuknicama, dodano radi jasnoće.

383 RS29 prethodno navodi da:
„Sukladnost s kodeksom ponašanja (članak 40) se mora uzeti u obzir (članak 35(8)) prilikom procjenjivanja učinka postupaka obrade podataka. To može biti korisno da dokaže da su primjerene mjere odabrane ili ustanovljene, pod uvjetom da je kodeks ponašanja prikladan postupku obrade. Certificiranja, pečati i oznake u svrhe dokazivanja sukladnosti s GDPR-om postupaka obrade voditelja obrade i izvršitelja (članak 42), kao i Obvezujuća korporativna pravila (OKP), trebaju se također uzeti u obzir." RS Smjernice o PUZP-ima (bilješka 351, iznad), str. 16.

- identificiraju se prijetnje koje bi mogle voditi do nezakonitog pristupa, neželjenih izmjena i gubitka podataka;
- procjenjuju se vjerojatnost i težina (uvodna odredba 90);

- određuju se mjere predviđene za rješavanje tih rizika (članak 35(7)(d) i uvodna odreba 90);

- **uključuju se zainteresirane strane:**
  - traži se savjet od SZP-a (članak 35(2));
  - traži se mišljenje ispitanika ili njihovih predstavnika, kada je to primjereno (članak 35(9)).

ŠTO UČINITI S EVIDENCIJOM O PUZP-U

Prva i glavna svrha evidencije o PUZP-u (koja obuhvaća sve gornje "kriterije") je imati **dokaz** da je proveden ispravan, dubinski PUZP, sukladno GDPR-u (tj. udovoljeno je gornjim kriterijima).

Kada PUZP identificira istodobno i (visoke) rizike i mjere koje se mogu poduzeti da se riješe ti rizici, a koje su "prikladne" uzimajući u obzir vjerojatnost i težinu rizika i troškove mjera, i kada su takve mjere doista odobrene i usvojene (pri čemu su i to odobrenje i usvajanje također evidentirani), evidencija o PUZP-u može pružiti **važan "element" u cjelokupnom dokazivanju sukladnosti i "**posebna sredstva" za to (iako navedeno ne predstavlja zakonsku pretpostavku usklađenosti), i općenito (premda će SZP i dalje morati kontinuirano **provjeravati i pratiti** da se mjere za ublažavanje rizika nastavljaju primjenjivati i nastavljaju biti odgovarajuće u svjetlu praktičnog, organizacijskog i tehnološkog razvoja: vidi pod ovom Zadaćom, pod naslovom "*Kontinuirano praćenje sukladnosti*").

Primjeri slučajeva kada je PUZP identificirao i visoke rizike i mjere za ublažavanje rizika, koji su smatrani *(in casu*, od strane EuroPrise) dostatnima da se dopusti obrada. Posljedično, oba slučaja bi omogućila voditelju obrade da pouzdano zaključi kako ishod PUZP-a pokazuje da obrada NE bi trebala biti predana nadležnom TZP-u radi savjetovanja:[384]

1. ***Agencija za socijalnu skrb koristi glasovnu biometrijsku autentifikaciju zbog sprječavanja prijevare sa socijalnim pravima.***

Identifikacija rizika: kako je istaknuo RS29, tri glavna rizika nastala korištenjem biometrijskih podataka su: (i) činjenica da su biometrijska svojstva osobe nezamjenjiva (što znači da se alat za autentifikaciju koji se zasniva na sirovim biometrijskim podacima, ako se jednom izgubi, više ne može zamijeniti); (ii) lakoća kojom se biometrijski podaci mogu koristiti radi uparivanja različitih skupina podataka; i (iii) mogućnost da se biometrijski podaci mogu dobiti potajno (kradom).

Mjere za ublažavanje rizika: Kod (glasovnog) biometrijskog autentifikacijskog alata, koji se koristi za borbu protiv prijevare oko socijalnih prava, koristi se jedinstveni glasovni obrazac, koji se stvara iz izvornih ("sirovih") biometrijskih podataka, a ne sami sirovi podaci, koji se uništavaju nakon upisivanja ispitanika. Glasovni obrazac je jedinstven za bilo koju posebnu aktivaciju, te se ne može koristiti za

384 Ovi primjeri su uzeti iz proizvoda koji se dobili Privacy Seal, s pravnim procjenama koje je izradio Douwe Korff, vidjeti: https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (četvero-faktorski autentifikacijski alat koji uključuje biometrijsko rješenje); https://www.european-privacy-seal.eu/eps-en/valid-pos (alat koji spaja lokaciju sumnjive bankarske transakcije s lokacijom mobilnog telefona nositelja kartice). U procjenama, oba su proizvoda hvaljena zbog svoje iznimne minimizacije podataka i svojstava tehničke zaštite podataka, te radi načina na koji su ublažavale rizike povezane s, odnosno korištenje biometrijskih podataka i provjere lokacije.

ponovno stvaranje izvornih (sirovih) biometrijskih podataka. To se dotiče svih triju gore navedenih rizika: (i) ako bi glasovni obrazac bio kompromitiran, novi, različiti se može stvoriti vrlo jednostavno (uz pomoć ispitanika, kojeg bi trebalo ponovo upisati); (ii) različiti glasovni obrasci korišteni za različite aktivacije istog alata ne mogu se upariti jedan s drugim ni s drugim glasovnim podacima ili glasovnim obrascima; i (iii) glasovni obrazac se kreira prilikom procesa upisa licem-u-lice.

2. ***Financijska institucija provjerava lokaciju mobilnog telefona klijenta kako bi vidjela je li (ugrubo) na istom mjestu kao i bankovna kartica klijenta (koja se koristi za transakciju koja je alarmirana kao sumnjiva).***

Identifikacija rizika: Precizni detalji nečije lokacije u određenom trenutku mogu biti nadasve otkrivajući u smislu osjetljivih pitanja, a otkrivanje tih detalja stoga predstavlja ozbiljno miješanje u privatnost i privatni život dotičnog pojedinca – kako je Europski sud za ljudska prava potvrdio u slučaju *Naomi Campbell*.[385]

Mjere za ublažavanje rizika: Kod alata za sprečavanje prijevare bankovnom karticom, lokacijski podaci na mobilnom telefonu su reducirani, čak i prije prijenosa na korisnika tog alata (financijske institucije), na vrlo grubo određeno područje, obično državu ili saveznu državu. Ovo je dostatno da alat radi učinkovito (tj. da je u mogućnosti utvrditi dostatnom sigurnošću je li dotična transakcija autentična ili prijevarna), istodobno smanjujući nametljivost provjere lokacije na apsolutan minimum.

Evidencija se također može učiniti dostupnom (ili se može na nju pozvati) kod **savjetovanja** koje uključuje stranke ili građane, ili u odgovoru na **upite i pritužbe ispitanika i nevladinih organizacija** koje predstavljaju ispitanike (ili medija). U tom smislu, RS29 napominje da:[386]

Objava PUZP-a nije zakonski uvjet GDPR-a, već je odluka voditelja obrade hoće li to učiniti. Međutim, voditelji obrade bi trebali razmotriti objaviti barem dijelove, kao što je recimo sažetak ili zaključak njihovog PUZP-a.

Svrha je takvog procesa pomoći usvojiti povjerenje u postupke obrade voditelja, te dokazati pouzdanost [odgovornost] i transparentnost. ***Posebno je dobra praksa objaviti PUZP u slučajevima kada su članovi javnosti dotaknuti postupkom obrade. To bi posebno mogao biti slučaj kada javno tijelo provodi PUZP.***

Objavljeni PUZP ne treba sadržavati cjelokupnu procjenu, posebno kada bi PUZP mogao iznositi specifične informacije koje se tiču sigurnosnih rizika za voditelja obrade ili odati poslovne tajne ili komercijalno osjetljive informacije. U tim okolnostima, objavljena verzija bi se mogla sastojati samo od sažetka glavnih zaključaka PUZP-a, ili čak samo od izjave da je PUZP bio proveden.

Evidencija o PUZP-u je od posebne važnosti kod rješavanja bilo kojih upita koje postavi TZP, bilo da djeluju u svojem svojstvu općeg nadzora ili vezano za rješavanje pritužbe.

Konkretnije, kada PUZP identificira istodobno i (visoke) rizike i ustanovi da **ne postoje** mjere koje bi se mogle poduzeti da se dostatno riješe ti rizici (ili barem da ne postoje mjere koje su "prikladne" uzimajući u obzir

385 ECtHR, MGN v. the UK, presuda od 18. siječnja 2011, dostupno na: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-102965%22]}
RS Smjernice o procjeni učinka na zaštitu podataka (bilješka 315, gore) str. 18, naglasak u podebljanim slovima izvoran, naglasak u kurzivu i podebljanim slovima dodan.

386 RS Smjernice o procjeni učinka na zaštitu podataka (bilješka 315, gore) str. 18, naglasak u podebljanim slovima izvoran, naglasak u kurzivu i podebljanim slovima dodan.

vjerojatnost i težinu rizika i troškove mjera), voditelj obrade se mora **savjetovati s TZP-om** (čl. 36) – a **evidencija relevantnog PUZP-a mora se uručiti TZP-u:**[387]

> kada PUZP otkrije visoke rezidualne rizike, voditelj obrade je dužan zatražiti prethodno savjetovanje za obradu od nadležnog tijela (članak 36(1)). Kao dio ovoga, PUZP se mora dostaviti u cijelosti (članak 36(3)(e)). Nadzorno tijelo može pružiti savjet,[388] te neće kompromitirati poslovne tajne ili otkriti sigurnosne ranjivosti, uz primjenu načela važećih u svakoj Državi članici za javni pristup službenim dokumentima.

Države članice mogu također, sukladno svojem **nacionalnom pravu**, zatražiti voditelje obrade da se savjetuju s TZP-om "u pogledu obrade koju obavlja voditelj obrade za izvršenje zadaće koju voditelj obrade provodi u javnom interesu, uključujući i obradu u vezi sa socijalnom zaštitom i javnim zdravljem" (čl. 36(5)), a ovo je učinjeno za ove potonje slučajeve u npr. Francuskoj i Italiji.

Ako TZP nije zadovoljan informacijama u PUZP evidenciji (i/ili informacijama dobivenima na drugi način), TZP može **narediti** voditelju obrade da pruži sve daljnje informacije koje smatra potrebnima za procjenu predmeta (usp. čl. 58(1)(a)).

Obično, TZP će pokušati **pomoći** voditelju obrade u nalaženju rješenja – tj. identificirati mjere koje bi primjereno umanjile identificirane (visoke) rizike (po mišljenju nadzornog tijela), a pod uvjetom da se voditelj obrade usuglasi usvojiti te mjere (te da njihovo usvajanje i nastavak korištenja budu provjereni i praćeni od strane SZP-a), to bi riješilo stvar (kako i SZP treba evidentirati, te će također evidentirati i nadzorno tijelo).

Ali, alternativno, nadzorno tijelo može izdati **naredbu** voditelju obrade, tražeći od njega da usvoji specifične mjere za predložene postupke obrade (usp. čl. 58(2)(d)), ili doista **zabraniti** predloženu obradu (čl. 58(2)(f)).

SZP bi, naravno, opet trebao bilježiti bilo koje takve naredbe, te kontinuirano provjeravati da ih se poštuje (te bilježiti svoje zaključke). Ali, kao i uvijek, osim ove provjere, praćenja i evidentiranja, na kraju je voditelj obrade taj koji će odgovarati za bilo koji propust u smislu sukladnosti.

387 Idem.
388 Pisani savjet voditelja obrade je nužan jedino kada je nadzorno tijelo mišljenja da namjeravana obrada nije u skladu uredbom prema članku 36(2).

PRAĆENJE SUKLADNOSTI (UKLJUČUJUĆI ISTRAŽIVANJE PRITUŽBI):

5. ZADAĆA: Kontinuirano ponavljanje zadaća 1. – 3. (i 4.)

Kako navodi RS29 u svojim Smjernicama o SZP-ima (što podržava EOZP), članak 39(1)(b) povjerava SZP-u, između ostalih obveza, i obveza "praćenja" poštivanja [sukladnosti]" svoje organizacije s odredbama GDPR-a, a Uvodna odredba 97 dalje navodi da [bi] SZP "trebao pomagati voditelju obrade ili izvršitelju obrade pri praćenju unutarnje usklađenosti s ovom Uredbom".[389] Kako sam izraz "praćenje" ukazuje, to nije jednokratna, već je kontinuirana odgovornost.

Međutim, u skladu s našom raspravom o ulozi SZP-a u 2. dijelu, pod točkom 2.3.4, prethodno u tekstu, RS29 također (ponovo) naglašava da ovo:[390]

> Ne znači da je SZP taj koji je osobno odgovoran kada se javi slučaj nesukladnosti. GDPR jasno navodi da je voditelj obrade, a ne SZP, taj od kojeg se traži da "*provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom*" (članak 24(1)). Sukladnost zaštite podataka je korporativna odgovornost voditelja obrade, a ne SZP-a.

RS29 nastavlja kako u okviru dijela ovih obveza praćenja sukladnosti, SZP može posebice na kontinuiranoj osnovi:

- prikupiti informacije da bi identificirao aktivnosti obrade,
- analizirati i provjeriti sukladnost aktivnosti obrade, i
- informirati, savjetovati i izdavati preporuke voditelju obrade i izvršitelju obrade.

Kako bilježi u odnosu na PUZP (4. zadaće):[391]

> Treba biti naglašeno da u cilju upravljanja rizicima za prava i slobode pojedinaca, rizici moraju biti identificirani, analizirani, procijenjeni, tretirani (npr. ublaženi…) **te redovito preispitani**.

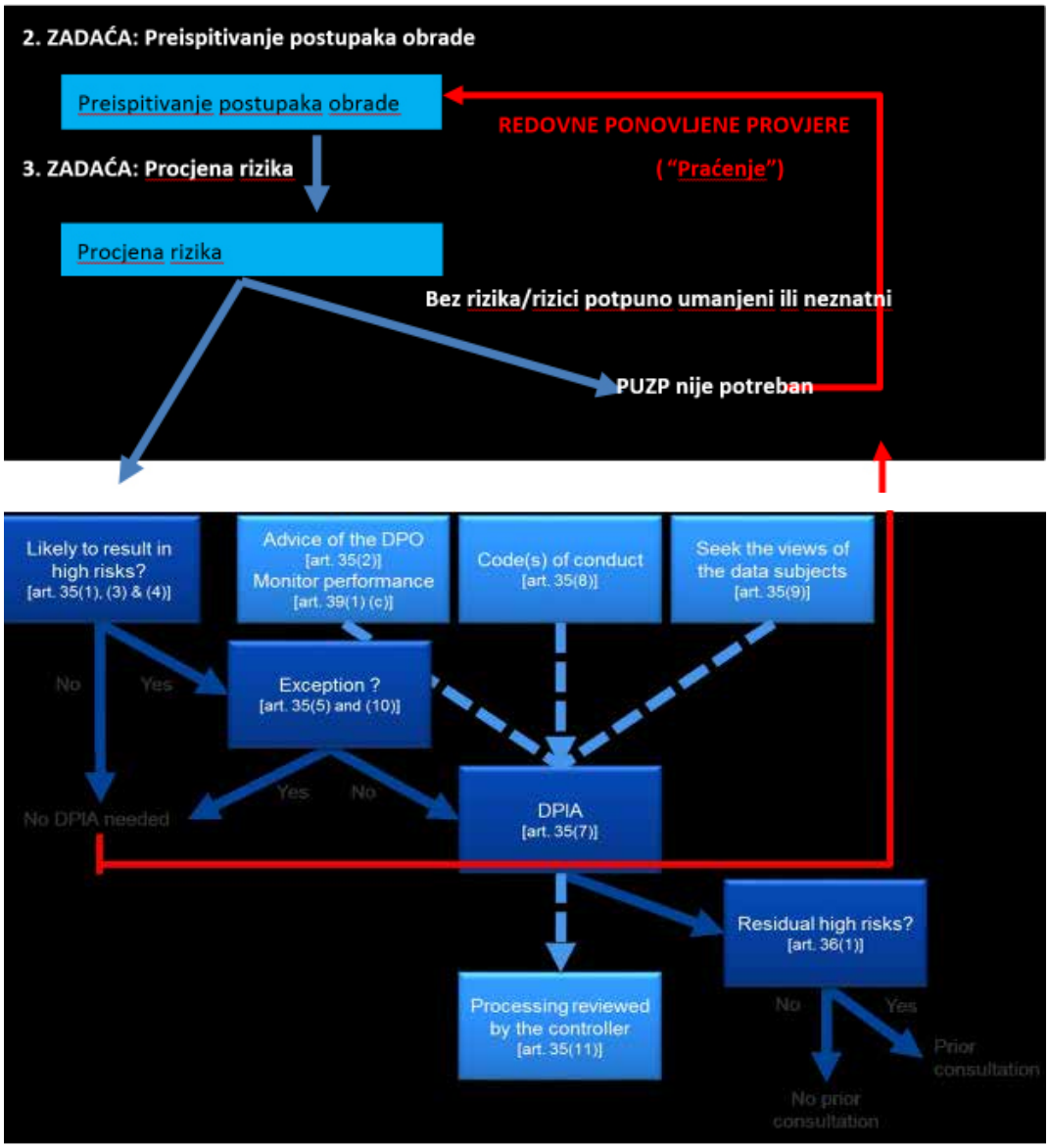
Drugim riječima, zadaće 1. - 4., prethodno u tekstu (ili ako ne postoje "visokorizične" obrade, onda zadaće 1. - 3.), se trebaju ponavljati na kontinuiranoj osnovi, posebice naravno ako organizacija promijeni bilo koji postupak obrade osobnih podataka, ili primijeni bilo koje nove. Kako navodi ENZP (u svojem savjetu SZP-ovima europskih institucija):[392]

> Vaše evidencije moraju odražavati stvarnost Vaših [odnosno, Vaše institucije] postupaka obrade. To znači da Vi morate osigurati da su isti ažurni. Kada [Vaša institucija] planirate promjene Vaših postupaka obade, provjerite treba li ažurirati evidenciju. Dobra je ideja formalno uključiti ovu provjeru u Vaš promijenjeni proces upravljanja. Također bi mogla biti dobra ideja provoditi redovita provjeravanja neovisno o planiranim promjenama kako biste otkrili promjene koje su možda ostale neprimijećene.

RS29 je ilustrirao ovaj posljednji dio niza u korisnom dijagramu, reproduciranom na sljedećoj strani, s dodanim ranijim stadijima (zadaće 2 i 3).

389 RS29 Smjernice o SZP-ima (bilješka 242, iznad), odlomak 4.1, Monitoring compliance with the GDPR (Praćenje sukladnosti s GDPR-om), na str. 16,7.
390 Idem, izvornik u kurzivu (italic).
391 RS Smjernice o PUZP-ima (bilješka 351, iznad), bilješka 10 na str. 6, dodan naglasak.
392 EDPS, Accountability on the ground (bilješka 353, iznad).

Dijagram koji je izradio RS29 s koracima koje treba slijediti vezano za PUZP,[393] s ranijim koracima (2. i 3. zadaća) dodanim na vrhu dijagrama:



Bilješka: Izuzeća sukladno čl. 35(5), opisana u dijagramu RS29, odnose se na nacionalnu sigurnost, obranu, sprječavanje kriminala, itd. Čl. 35(10) tiče se odredbe da nikakav PUZP nije potreban u odnosu na obradu propisanu zakonom, ako je opći PUZP za tu obradu već proveden u postupku donošenja zakona (što ne uključuje SZP).

Kao dio svojih obveza "praćenja poštivanja [sukladnosti]", SZP bi također trebao osigurati da je uvijek upoznat s bilo kojim promjenama u regulatornom i ugovornom (itd.) okviru unutar kojeg njegova/njena organizacija posluje, kako je istraženo u preliminarnoj zadaći (0. zadaća), tako da SZP ima mogućnost prepoznati učinak bilo kojih takvih promjena za (kontinuirana zakonitost i sukladnost GDPR-u) postupke obrade osobnih podataka njegove/njene organizacije, te može dati prikladan savjet relevantnim osobama u svojoj organizaciji (uključujući vodeće osobe iz uprave, kada je to primjenjivo).

Doista, SZP bi trebao – kad god je to primjenjivo, zajedno s drugim SZP-ovima u svojoj mreži SZP-a i/ili s TZP-om, te uz savjetovanje sa svojim vodećim osobama iz uprave – povremeno biti voljan usvojiti pozicije i gledišta o predloženim ili sugeriranim promjenama u tom okviru, kao što su prijedlozi vlade da organizacije kakva je upravo SZP-ova trebaju biti tražene, treba im biti omogućeno ili ih poticati da dijele određene osobne podatke za nove svrhe.

393 RS Smjernice o PUZP-ima (bilješka 351, iznad), str. 7.

6. ZADAĆA: *Rješavanje povreda osobnih podataka*

Dvije glavne, važne inovacije koje je donio GDPR u usporedbi s Direktivom o zaštiti podataka iz 1995., jesu: (i) opći zahtjev obavijestiti relevantni (tj. "nadležno") TZP o bilo kojim povredama osobnih podataka koje mogu dovesti do rizika za prava i slobode pojedinaca; i (ii) obveza obavijestiti ispitanike o takvim povredama u slučajevima gdje postoji vjerojatnost da će povreda rezultirati "visokim rizikom" u odnosu na prava i slobode fizičkih osoba.

Radna skupina iz čl. 29 je izdala detaljne smjernice o tome kako treba postupati s povredama osobnih podataka;[394] a ove smjernice je podržao i Europski odbor za zaštitu podataka na svojem prvom sastanku.[395] Rasprava, niže u tekstu, se opširno nadograđuje na tim smjernicama i poziva na njih. Navedeni primjeri su također uzeti iz tih Smjernica RS29.[396] **Obavještavanje relevantnog TZP-a:**

Ideja obavještavanja o povredama osobnih podataka nije nova. Kako je opisano pod točkom 1.3.3, prethodno u tekstu,[397] obveza obavještavanja o povredi osobnih podataka bila je već uključena i u Direktivu o e-privatnosti. Međutim, ta obveza je bila ograničena na pružatelja elektroničkih komunikacijskih mreža, odnosno pružatelje usluga.[398] GDPR koristi istu definiciju "*povrede osobnih podataka*" kakva je sadržana i u Direktivi o e-privatnosti, ali bez ovog ograničenja:

> kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani (čl. 4(12)).[399]

Smjernice RS29 razjašnjavaju donekle detaljno što bi trebali značiti relevantni izrazi, te navodi različite vrste povreda osobnih podataka ("*povreda povjerljivosti*"; "*povreda integriteta*"; "*povreda dostupnosti*")[400]

Primjeri

Primjer gubitka osobnih podataka može uključivati gubitak ili krađu uređaja koji sadrži primjerak baze podataka klijenata voditelja obrade. Daljnji primjer može biti kada je jedini primjerak niza osobnih podataka enkriptiran ucjenjivačkim softverom, tzv. *ransomware* (zlonamjerni softver koji enkriptira podatke voditelja obrade sve dok se ne plati traženi iznos ucjene), ili ga je enkriptirao voditelj obrade koristeći ključ kojeg više ne posjeduje.

Primjeri gubitka dostupnosti kada su podaci obrisani ili slučajno ili ih je obrisala neovlaštena osoba, ili, u primjeru sigurno enkriptiranih podataka, ključ za dešifriranje je izgubljen. U slučaju da voditelj obrade ne može obnoviti pristup podacima, primjerice, iz sigurnosne kopije (*backup*), tada se to smatra trajnim gubitkom dostupnosti.

Gubitak dostupnosti može se također dogoditi kada se javi značajan poremećaj uobičajene usluge neke organizacije, primjerice, nestanak električne energije ili napad uskraćivanjem resursa (*denial of service attack*), čime osobni podaci postaju nedostupni.

394 RS29, Guidelines on Personal data breach notification under Regulation 2016/679 (RS250 rev. 01, usvojeno 3. listopada 2017., s posljednjom revizijom i usvojeno 6. veljače 2018. (dalje u tekstu: "RS29 Guidelines on Data Breach Notification" ili, u ovom odlomku, jednostavno "the RS29 Guidelines"), dostupno na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [400] Vidi bilješku 248, prethodno.
395 Vidi bilješku 248, prethodno.
396 RS29 Smjernice također raspravljaju o obvezama obavješćivanja prema drugim zakonskim instrumentima: vidi Odlomak VI Smjernica. O tome se dalje ne govori ovdje.
397 U pododlomku "*Key features of the e-Privacy Regulation*", pod podnaslovom "Data breach notification".
398 Kako se navodi u Uvodu u RS29 Smjernice, neke Države članice su također već imale proširene zahtjeve obavješćivanja o povredi podataka.
399 Direktiva o e-privatnosti je dodala neke riječi nakon ovih, konkretno riječi: "*vezano za pružanje javno dostupnih elektroničkih komunikacijskih usluga u Zajednici*" (čl. 2(i)).
400 RS29 Smjernice, str. 7, s pozivom na prethodno (2014) RS29 Mišljenje o obavješćivanju o povredi.

Čak i privremeni gubitak dostupnosti može predstavljati povredu osobnih podataka:

Primjeri

U kontekstu bolnice, ako kritični medicinski podaci o pacijentima nisu dostupni, čak i privremeno, ovo bi moglo predstavljati rizik za prava i slobode pojedinaca; primjerice, operacije mogu biti otkazane i životi dovedeni u pitanje.

Za razliku od toga, u slučaju nedostupnosti sustava medijske kompanije u trajanju od nekoliko sati (npr. zbog nestanka električne energije), ako je ta kompanija spriječena slati biltene (*newsletters*) svojim pretplatnicima, malo je vjerojatno da će to predstavljati rizik za prava i slobode pojedinaca.

Zaraza zbog ucjenjivačkog softvera, tzv. *ransomware*, mogla bi dovesti do privremenog gubitka dostupnosti ako se podaci mogu vratiti iz sigurnosne kopije (*backup*). Međutim, napad na mrežu se i dalje dogodio, te bi mogla biti potrebna obavijest je li incident kvalificiran kao povreda povjerljivosti (tj. privatnim je podacima pristupio napadač) te ovo predstavlja rizik za prava i slobode pojedinaca.

Članak 33(1) navodi kako slijedi:

> U slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo nadležno u skladu s člankom 55. o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje (članak 33(1)).

Izvršitelj obrade "*bez nepotrebnog odgađanja izvješćuje voditelja obrade nakon što sazna za povredu osobnih podataka*" (čl. 33(2)). RS29 preporučuje da izvršitelj obrade:

> što prije izvijesti voditelja obrade, s daljnjim informacijama o povredi koje dostavlja u fazama, kako što više pojedinosti postane dostupno. Ovo je važno kako bi se pomoglo voditelju obrade da zadovolji uvjete obavješćivanja nadzornog tijela unutar 72 sata. (RS29 Smjernice, str. 14) smatrat će se da je voditelj obrade "**svjestan**" povrede kad ga izvršitelj obrade obavijesti o tome;[401] a voditelj obrade mora onda obavijestiti TZP (kako je spomenuto), osim ako se primjenjuje *caveat* da povreda podataka vjerojatno neće prouzročiti rizik za prava i slobode pojedinaca.

U nekim slučajevima, izvršitelj obrade može nastupati za određen broj – moguće čak i velik broj – različitih voditelja obrade, primjerice kao pružatelj usluge pohrane podataka u oblaku. RS29 savjetuje kako slijedi u tim situacijama:

> Kada izvršitelj obrade pruža usluge više voditelja obrade koji su svi pogođeni istim incidentom, izvršitelj obrade će morati obavijestiti svakog voditelja obrade o incidentu.
>
> Izvršitelj obrade bi mogao izvijestiti u ime voditelja obrade, ako je voditelj obrade dao valjano ovlaštenje izvršitelju obrade i ako je to dio ugovorenog dogovora između voditelja i izvršitelja obrade. Takvo izvješćivanje mora biti obavljeno sukladno člancima 33 i 34. Međutim, važno je primijetiti da zakonska odgovornost obavješćivanja i dalje ostaje na voditelju obrade (str. 14).

401 RS Smjernice, str. 14.

Obavješćivanje o povredi podataka relevantnom ("nadležnom") TZP-u[402] "mora … barem":

a. opisati prirodu povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
b. navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
c. opisati vjerojatne posljedice povrede osobnih podataka;
d. opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica (čl. 33(3)).

U tom smislu, RS29 kaže da voditelj obrade može:[403]

Ako je potrebno, odabrati pružiti daljnje pojedinosti. Različite vrste povreda (povjerljivost, integritet ili dostupnost) mogu zahtijevati dostavljanje dodatnih pojedinosti kako bi se u cijelosti objasnile okolnosti svakog pojedinog slučaja.

Primjer

Kao dio svojeg obavješćivanja nadzornog tijela, voditelj obrade može smatrati korisnim imenovati izvršitelja obrade ako je on u korijenu uzroka povrede, posebno ako je to dovelo do incidenta koji utječe na evidenciju osobnih podataka mnogih drugih voditelja obrade koji koriste istog izvršitelja obrade.

U svakom slučaju, nadzorno tijelo može zahtijevati daljnje pojedinosti kao dio svoje istrage povrede.

Štoviše:

Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružati bez nepotrebnog daljnjeg odgađanja, i to u mjeri u kojoj nije moguće pružiti informacije u isto doba, informacije se mogu pružiti u fazama bez nepotrebnog daljnjeg odgađanja (čl. 33(4)).[404]

Primjer

Voditelj obrade obavijesti nadzorno tijelo unutar 72 sata od otkrivanja povrede kojom je izgubio USB memorijski ključ koji sadrži kopiju osobnih podataka nekih od njegovih klijenata. USB memorijski ključ se kasnije pronađe jer je zabunom spremljen na pogrešno mjesto unutar prostorija voditelja obrade i vraćen je. Voditelj obrade ažurira informacije, tj. obavještava nadzorno tijelo i zahtijeva izmjenu obavijesti.

VRIJEME OBAVJEŠĆIVANJA:

RS29 Smjernice pojašnjavaju kada se može reći da je voditelj obrade (ili izvršitelj) postao "**svjestan**" povrede podataka i naglašava da također postoje obveze predvidjeti i pripremiti se za takav događaj:[405]

402 Za smjernice o obavještavanju o prekograničnim povredama i o povredama koje se dogode izvan EU, vidi odlomak C RS29 Smjernicama (str. 16-18).
403 RS29 Smjernice, str. 15.
404 Za detalje i daljnje smjernice o ovom pitanju, vidi RS29 Smjernice, str. 15-16.
405 RS29 Smjernice, str. 10-11.

Kako je detaljno prethodno opisano, GDPR zahtijeva da, u slučaju povrede, voditelj obrade obavijesti o povredi bez nepotrebnog odgađanja i to, kada je to izvedivo, unutar najviše 72 sata nakon što sazna za povredu. Ovo može iznjedriti pitanje o tome kada se može smatrati da je voditelj obrade postao "svjestan" povrede. RS29 drži da se treba smatrati da je voditelj obrade postao "svjestan" kada taj voditelj obrade ima razuman stupanj sigurnosti da se sigurnosni incident dogodio koji je doveo do kompromitiranja osobnih podataka.

Međutim, kako je prethodno navedeno, GDPR zahtijeva da voditelj obrade primijeni sve odgovarajuće tehničke zaštitne i organizacijske mjere kako bi utvrdio odmah je li se povreda dogodila i što prije obavijestio nadzorno tijelo i ispitanike. Također navodi da se činjenica da je obavijest dana bez nepotrebnog odgađanja treba utvrditi uzimajući u obzir posebice prirodu i težinu povrede, kao i njene posljedice i negativne učinke za ispitanika. Time se stavlja obveza na voditelja obrade osigurati da će biti "svjesni" bilo kojih povreda pravovremeno tako da mogu poduzeti odgovarajuće radnje.

Kada se točno može smatrati da je voditelj obrade "svjestan" određene povrede, ovisit će o okolnostima dotične povrede. U nekim slučajevima, bit će relativno jasno od samog početka da je došlo do povrede, dok će u drugim slučajevima, moguće biti potrebno neko vrijeme da se ustanovi jesu li osobni podaci kompromitirani. Međutim, naglasak treba biti stavljen na brzo reagiranje kako bi se istražio incident da bi se utvrdilo je li doista došlo do povrede osobnih podataka, a ako jest tako, da bi se poduzele radnje za ispravljanje i obavješćivanje, ako je potrebno.

Primjeri

1. U slučaju gubitka USB memorijskog ključa s neenkriptiranim osobnim podacima, često nije moguće utvrditi jesu li neovlaštene osobe dobile pristup tim podacima. Neovisno o tome, premda voditelj obrade možda nije u mogućnosti ustanoviti je li se dogodila povreda povjerljivosti, o takvom se slučaju mora izvijestiti jer postoji razuman stupanj sigurnosti da je došlo do povrede dostupnosti; voditelj obrade bi postao "svjestan" kada je shvatio da je USB memorijski ključ izgubljen.

2. Treća strana obavijesti voditelja obrade da su slučajno dobili osobne podatke jednog od njegovih klijenata i pruži dokaze neovlaštenog otkrivanja. S obzirom da je voditelju obrade prezentiran jasan dokaz povrede povjerljivosti, nema sumnje da je time postao "svjestan" povrede.

3. Voditelj obrade primijeti da je došlo do mogućeg upada u njegovu mrežu. Voditelj obrade provjerava svoje sustave da bi utvrdio jesu li osobni podaci koji se čuvaju u tom sustavu bili kompromitirani i potvrđuje da se upravo to dogodilo. Ponovno, s obzirom da voditelj obrade sada ima jasne dokaze o povredi, nema sumnje da je postao "svjestan" povrede.

4. Kibernetički kriminalac kontaktira voditelja obrade nakon što je hakirao njegov sustav kako bi tražio otkupninu. U tom slučaju, nakon provjere svojeg sustava kako bi utvrdio da je isti bio napadnut, voditelj obrade ima jasne dokaze da se povreda dogodila i nema sumnje da je time postao svjestan iste.

5. Pojedinac (neka osoba) obavijesti voditelja obrade da je dobio e-poštu kojom se netko lažno predstavlja kao voditelj obrade, a sadrži osobne podatke koji se odnose na pojedinčevo (stvarno) korištenje usluge voditelja obrade, sugerirajući da je došlo do kompromitiranja sigurnosti voditelja obrade. Voditelj obrade provodi kratku istragu i identificira upad u svoju mrežu i dokaze neovlaštenog pristupa osobnim podacima. Voditelj obrade bi se sada smatrao "svjesnim" povrede i potrebno je izvješćivanje nadzornog tijela osim ako nije vjerojatno da će prouzročiti rizik za prava i slobode pojedinaca. Voditelj obrade će trebati poduzeti odgovarajuće radnje da bi postupio po povredi.

DOKUMENTIRANJE I PROCJENA POVREDE:

GDPR također propisuje da:

> Voditelj obrade dokumentira **sve** povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštovanja ovog članka (čl. 33(5), uz dodan naglasak).

Podsjećamo da se ovaj potonji zahtjev odnosi na **sve** ("bilo koju") povrede osobnih podataka: nije ograničen na povrede osobnih podataka o kojima TZP mora biti obaviještenom tj. evidencija također mora uključivati bilo koje povrede podataka za koje je (po mišljenju voditelja obrade) "vjerojatno neće prouzročiti rizik za prava i slobode pojedinaca".

U praksi, SZP će morati biti blisko i duboko uključen u ova pitanja. Često, sumnja na povredu će vjerojatno biti prvo prijavljena interno SZP-u (i/ili glavnom nadležnom za tehnologiju ili sigurnost) – a SZP mora onda (ovisno o slučaju, s tim drugim službenicima) načiniti prvu, trenutnu procjenu barem sljedećih pitanja:

- je li se doista dogodila povreda osobnih podataka kako je definirana u GDPR-u (vidi definiciju u članku 4(12), prethodno citirano)

  i *ako se utvrdi da je doista došlo do povrede ili je vjerojatno da je moglo doći do povrede:*
- koje (kategorije) ispitanika jesu ili su mogle biti pogođene povredom i koje (kategorije) osobnih podataka su moguće izgubljene ili na drugi način pogođene

  NB: RS29 preporučuje da se te kategorije prijave TZP-u kod bilo kojeg obavješćivanja o povredi, i uistinu da: [406]

  Ako vrste ispitanika ili vrste osobnih podataka naznačuju rizik konkretne štete koja se javlja kao posljedica povrede (npr. krađa identiteta, prijevara, financijski gubitak, prijetnja ili profesionalna tajna), tada je važno da obavijest navodi te kategorije. Na taj način, to je povezano sa zahtjevom opisivanja vjerojatnih posljedica povrede.

  i *uzimajući te stvari u obzir:*
- je li "vjerojatno" ili "nije vjerojatno" da će povreda dovesti do rizika za prava i slobode pojedinaca

  RS29 raspravlja pitanje kada to obavijest nije potrebna donekle detaljno[407] i daje sljedeći primjer:

> **Primjer**
>
> Povreda za koju nije potrebno obavješćivanje nadzornog tijela bila bi gubitak sigurnosno enkriptiranog mobilnog uređaja, kojeg koristi voditelj obrade i njegovo osoblje. Pod uvjetom da enkripcijski ključ ostane unutar sigurnog posjeda voditelja obrade i da to nije jedina kopija osobnih podataka, tada bi osobni podaci bili nedostupni napadaču. To znači da povreda vjerojatno ne bi dovela do rizika za prava i slobode ispitanika u tom slučaju. Ako kasnije postane očigledno da je enkripcijski ključ kompromitiran ili da je enkripcijski softver ili algoritam ranjiv, tada će se rizik za prava i slobode pojedinaca izmijeniti, te stoga obavješćivanje možda sada bude potrebno.

i *ali ako je procjena da **postoji** vjerojatnost takvog potencijalnog rizika:*

- je li rizik "visok rizik za prava i slobode [tih] pojedinaca" (zato što bi to zahtijevalo ne samo obavještavanje o povredi TZP-a, već također i obavještavanje ispitanika, kako je opisano pod sljedećim podnaslovom).[408]

406 RS29 Smjernice, str. 14.
407 RS29 Smjernice, str. 18-19. Vidjeti netaksativan popis primjera u prilogu (Prilog B) uz Smjernice, reproduciran dalje u tekstu, pod sljedećim podnaslovom.
408 Vidi posebno diskusiju pod podnaslovom "*Assessing risk and high risk*".

Kako RS29 naglašava, važnost imati mogućnost identificirati povredu, procijeniti rizik za pojedince i potom obavijestiti tijelo ako je potrebno, naglašena je u Uvodnoj odredbi 87 GDPR-a:

> Trebalo bi se utvrditi jesu li provedene sve odgovarajuće mjere tehničke zaštite i organizacijske mjere da bi se odmah utvrdilo je li došlo do povrede osobnih podataka i odmah obavijestilo nadzorno tijelo i ispitanika. Trebalo bi utvrditi činjenicu je li obavijest pružena bez nepotrebnog odgađanja posebno uzimajući u obzir prirodu i ozbiljnost povrede osobnih podataka i njezine posljedice i negativne učinke za ispitanika. Takva obavijest može dovesti do intervencije nadzornog tijela u skladu s njegovim zadaćama i ovlastima predviđenima ovom Uredbom.

I naravno, ako procjene ukazuju na to da je došlo do povrede, te da postoje rizici za interese pojedinaca, tada treba hitno zatražiti **mjere za ublažavanje rizika**.

Gornja pitanja bi trebala također **hitno, čim prije bude moguće**, proslijediti najvišoj razini uprave. Doista, bilo koje interne diskusije o gornjim pitanjima ne bi smjele odugovlačiti obavještavanje najviše razine uprave čim se utvrdi da je došlo do povrede.

Činjenica da su te procjene učinjene savjesno, trebala bi biti **pažljivo evidentirana**,[409] zajedno s ishodima relevantnih procjena i razlozima za te procjene; razmotrenim mjerama za ublažavanje rizika; činjenicom da su procjene i predložene mjere za ublažavanje rizika prenesene najvišoj razini uprave; stvarnim mjerama koje je odobrila uprava i ovisno o tome jesu li provedene, kada su provedene; te naravno činjenicom da se o povredi (ako je utvrđeno da o njoj treba izvijestiti) obavijestio relevantni TZP i kada, uz presliku obavijesti; te kada je to bilo potrebno, činjenicom da su ispitanici obaviješteni, te kako, s preslikom relevantne obavijesti i bilo kojih relevantnih tiskovnih priopćenja itd. (kako se raspravlja pod sljedećim naslovom). Štoviše, kako RS29 Smjernice navode:

> Dokumentacija o povredi trebala bi se stvarati za vrijeme dok se stvar razvija (str. 12).

U organizacijama koje su imenovale SZP, on će imati važnu ulogu koju treba odigrati u tom smislu, kako i RS29 naglašava:[410]

> Voditelj obrade ili izvršitelj obrade mogu imati službenika za zaštitu podataka (SZP), bilo prema zahtjevima članka 37., ili dobrovoljno, kao izraz dobre prakse. Članak 39. GDPR-a popisuje niz obveznih zadaća za SZP, ali ne sprječava voditelja obrade u dodjeli dodatnih zadaća, ako je to prikladno.
>
> Od posebne važnosti za obavijest o povredi, obvezne zadaće SZP-a uključuju, između ostalih obveza, pružanje savjeta i informacija o zaštiti podataka voditelju obrade i izvršitelju obrade, praćenje sukladnosti s GDPR-om te pružanje savjeta u odnosu na PUZP. SZP mora također surađivati s nadzornim tijelom i djelovati kao kontaktna točka za nadzorno tijelo i za ispitanike. Treba također primijetiti da, kod obavješćivanja o povredi nadzornog tijela, članak 33(3)(b) traži od voditelja obrade da navede ime i kontaktne podatke svojeg SZP-a ili druge kontaktne osobe.
>
> U pogledu dokumentiranja povreda, voditelj obrade ili izvršitelj obrade mogu željeti pribaviti mišljenje svojeg SZP-a o pitanju strukture, osnivanju i vođenju ove dokumentacije. SZP-u bi se mogle također dodati zadaće vođenja takvih evidencija.
>
> Ovi čimbenici znače da bi SZP trebao odigrati ključnu ulogu kod pomaganja u sprječavanju ili tijekom pripreme za samu povredu pružajući savjete i prateći sukladnost, kao i tijekom same povrede (tj. prilikom

409 RS29 sugerira da se ovo učini "*u izvještajnom planu o incidentu voditelja obrade i/ili aranžmanima*" (str. 12). O ovome se dalje raspravlja donekle detaljno u RS29 Smjernicama, Odjeljak V, "*Accountability and recordkeeping*".
410 RS29 Smjernice, Odlomak V.B, str. 27-28.

> obavješćivanja nadzornog tijela) te tijekom bilo koje naknadne istrage od strane nadzornog tijela. U tom svjetlu, RS29 preporučuje da se SZP odmah obavijesti o postojanju povrede i da bude uključen tijekom rješavanja povrede i postupka obavješćivanja.

RS29 Smjernice jasno navode da organizacije ne bi samo trebale reagirati u ovom pogledu. Umjesto toga, trebaju imati pripremljenu **politiku sigurnosti** koja ***unaprijed*** ima namjeru izbjeći bilo koje povrede osobnih podataka te sadrži planove za sprječavanje, ublažavanje i okončavanje takvih povreda. U odnosu na postupke obrade osobnih podataka za koje postoji vjerojatnost da će rezultirati "visokim rizikom" za interese pojedinaca, izrada takve politike (pravila) može biti dio relevantne procjene učinka na zaštitu podataka (kako se navodi pod 4. zadaćom, prethodno u tekstu).[411]

OBAVJEŠTAVANJE ISPITANIKA:

RS29 pojašnjava zahtjeve obavještavanja ispitanika o povredi podataka kako slijedi:

U nekim slučajevima, osim obavješćivanja nadzornog tijela, voditelj obrade također mora obavijestiti o povredi i pogođene pojedince.

Članak 34(1) navodi:

> U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

Voditelji obrade bi se trebali prisjetiti da je obavješćivanje nadzornog tijela obvezno osim ukoliko nije vjerojatno da postoji rizik za prava i slobode pojedinaca kao rezultat neke povrede. Osim toga, kada je vjerojatno da će uslijed povrede doći do visokog rizika za prava i slobode pojedinaca, pojedinci također moraju biti obaviješteni. Prag za obavješćivanje pojedinaca o povredi je stoga viši negoli za obavješćivanje nadzornih tijela te se neće dakle za sve povrede tražiti obavješćivanje pojedinaca, time ih štiteći od nepotrebnog zamora obavijestima.

GDPR navodi da informiranje o povredi pojedinaca treba biti učinjeno "bez nepotrebnog odgađanja", što znači što je prije moguće. Glavni je cilj obavješćivanja pojedinaca pružiti im posebne informacije o koracima koje oni trebaju poduzeti kako bi zaštitili sami sebe. Kako je prethodno navedeno u tekstu, ovisno o prirodi povrede i nametnutom riziku, pravovremeno obavješćivanje će pomoći pojedincima da poduzmu korake kako bi se zaštitili od bilo kojih negativnih posljedica povrede.

Dodatak (Dodatak B) uz RS29 Smjernice, koji sadrži (netaksativan popis) 10 primjera povreda osobnih podataka i tko treba biti obaviješten, priložen je uz raspravu o sadašnjoj zadaći kao Prilog.

RS29 Smjernice dalje nastavljaju kako slijedi:[412]

Informacije koje se pružaju

Prilikom obavješćivanja pojedinaca, članak 34(2) navodi da:

> Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 33. stavka 3. točaka (b), (c) i (d).

411 RS29 Smjernice, str. 6.
412 Odlomak III.B, str. 20. Tekst uređen samo za prezentaciju.

Sukladno ovoj odredbi, voditelj obrade bi trebao barem pružiti sljedeće informacije:

- opis prirode povrede;
- ime i kontaktne podatke službenika za zaštitu podataka ili drugu kontaktnu osobu;
- opis vjerojatnih posljedica povrede; i
- opis poduzetih mjera ili predloženih mjera koje treba poduzeti voditelj obrade kako bi riješio povredu, uključujući, kada je to prikladno, mjere za ublažavanje njenih mogućih štetnih posljedica.

Primjer:

Kao primjer poduzetih mjera za rješavanje povrede i ublažavanje njenih mogućih negativnih učinaka, voditelj obrade može navesti da, nakon što je obavijestio o povredi relevantno nadzorno tijelo, voditelj obrade je dobio savjet o rješavanju povrede i umanjivanju njenog učinka. Voditelj obrade bi također trebao, kada je to prikladno, pružiti specifičan savjet pojedincima kako bi se zaštitili od mogućih negativnih posljedica povrede, kao što je resetiranje lozinke u slučaju kada su kompromitirane njihove pristupne autorizacije. Ponovno, voditelj obrade može odabrati pružiti i druge informacije povrh ovoga što je ovdje navedeno.

Smjernice također pojašnjavaju da:[413]

U načelu, o relevantnoj povredi bi pogođeni ispitanici trebali biti obaviješteni izravno, osim ako bi se time zahtijevao nerazmjeran napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način (čl. 34(3)c).

Takve obavijesti se ispitanicima trebaju pružiti "što je prije, u razumnim granicama, izvedivo i u bliskoj suradnji s nadzornim tijelom" (Uvodne odredbe 86). Kako navode Smjernice:[414]

Voditelji obrade mogu stoga željeti kontaktirati i zatražiti savjet nadzornog tijela, ne samo da bi tražili savjet o informiranju ispitanika o povredi sukladno članku 34., već također i o prikladnim porukama koje bi se slale ispitanicima, kao i o najprikladnijem obliku kontakta.

Vezan za to je i savjet sadržan u Uvodnoj odredbi 88 da bi obavijest o povredi trebala "uzeti u obzir legitimne interese tijela za izvršavanje zakonodavstva kada rano otkrivanje može nepotrebno naškoditi istrazi okolnosti povrede osobnih podataka". Ovo može značiti da u određenim okolnostima, kada je to opravdano, te prema savjetu tijela za izvršavanje zakonodavstva, voditelj obrade može odgoditi obavještavanje o povredi ugroženim pojedincima sve do doba kada to ne bi naškodilo takvim istragama. Međutim, ispitanici bi i dalje trebali biti ažurno obaviješteni nakon tog vremena.

Kad god nije moguće da voditelj obrade obavijesti o povredi pojedinca jer je nedovoljno podataka pohranjeno da bi se kontaktiralo pojedinca, u tim posebnim okolnostima, voditelj obrade bi trebao obavijestiti pojedinca čim bude razumno izvedivo to učiniti (npr. kada pojedinac iskoristi pravo iz članka 15. da pristupi osobnim podacima i pruži voditelju obrade potrebne dodatne informacije da ga se može kontaktirati).

413 Odlomak III.C, str. 21; Vidjeti za daljnje smjernice o alternativnim načinima obavješćivanja pogođenih ispitanika o povredi podataka.
414 *Idem*, str. 21-22.

Izuzeci:

Kako je navedeno u RS29 Smjernicama:[415]

Članak 34(3) spominje tri uvjeta koji, ako im je udovoljeno, ne zahtijevaju obavješćivanje pojedinaca u slučaju povrede. To su:

- Voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija.
- Odmah nakon povrede, voditelj obrade poduzeo je korake kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika. Primjerice, ovisno o okolnostima slučaja, voditelj obrade je moguće odmah identificirao i poduzeo mjere protiv pojedinca koji je pristupio osobnim podacima prije negoli je taj pojedinac bio u mogućnosti išta s time učiniti. Dužna pažnja i dalje treba biti posvećena mogućim posljedicama bilo koje povrede povjerljivosti, opet, ovisno o prirodi dotičnih podataka.
- Ako bi to uzrokovalo nerazmjeran napor da se kontaktiraju pojedinci, kada su njihovi kontaktni podaci izgubljeni uslijed povrede ili uopće nisu ni bili poznati. Primjerice, skladište ureda za statistiku je poplavljeno i dokumenti koji sadrže osobne podatke su bili pohranjeni samo u papirnom obliku. Umjesto toga, voditelj obrade mora obavijestiti javnost nekom javnom objavom ili poduzeti drugu sličnu mjeru, čime se pojedinci obavještavaju na jednako učinkovit način. U slučaju nerazmjernog napora, tehnički dogovori bi se također mogli predvidjeti da se pruže informacije o povrede, dostupno na zahtjev, što bi se moglo pokazati korisnim onim pojedincima koji su moguće pogođeni povredom, ali ih voditelj obrade ne može na drugi način kontaktirati.

Sukladno načelu pouzdanosti [odgovornosti], voditelji obrade bi trebali moći dokazati nadzornom tijelu da udovoljavaju jednom ili više od tih uvjeta. Treba imati na umu da dok na početku obavijesti ne moraju biti potrebne ako ne postoji rizik za prava i slobode pojedinaca, to se može s vremenom promijeniti i rizik mora biti ponovno procijenjen.

Ako voditelj obrade odluči ne obavijestiti pojedinca o povredi, članak 34(4) objašnjava da nadzorno tijelo može od njega to zahtijevati, ako smatra da bi povreda vjerojatno dovela do visokog rizika za pojedince. Alternativno, može smatrati da su uvjeti iz članka 34(3) udovoljeni, u kojem slučaju obavijest pojedincima nije potrebna. Ako nadzorno tijelo utvrdi da odluka o tome da se ne obavještava pojedince nije utemeljena, može razmotriti korištenje svojih dostupnih ovlasti i sankcija.

Procjenjivanje rizika i visokog rizika:

Ponovo, moglo bi biti dostatno citirati RS29 Smjernice:[416]

Premda GDPR uvodi obvezu obavještavanja o povredi, nije uvjet to učiniti u svim okolnostima:

- Obavijest nadležnom nadzornom tijelu se traži osim ako nije vjerojatno da će to dovesti do rizika za prava i slobode pojedinaca.
- Obavijest o povredi pojedincu se jedino aktivira kada je vjerojatno da će to dovesti do visokog rizika za njihova prava i slobode.

To znači da odmah nakon saznanja za povredu, od ključne je važnosti da voditelj obrade ne samo da bi trebao obuzdavati povredu, već bi također trebao procijeniti rizik koji bi mogao rezultirati iz iste. Postoje dva važna razloga za ovo: prvo, poznavanje vjerojatnosti i potencijalne težine učinka na pojedinca će pomoći voditelju obrade da poduzme učinkovite korake za obuzdavanje i rješavanje povrede; drugo, pomoći će mu da odredi je li obavijest nadzornom tijelu potrebna i, ako je to potrebno, je li potrebno obavješćivanje dotičnih pojedinaca.

415 Odlomak III.D, p. 22.
416 Odlomak IV.A i B, str. 23, reference ispuštene; ponovno donekle uređene za svrhe prezentacije.

Kako je prethodno objašnjeno, obavijest o povredi je potrebna, osim u slučaju kad nije vjerojatno da će to dovesti do rizika za prava i slobode pojedinaca, a ključni okidač koji zahtijeva obavješćivanje ispitanika o povredi je u slučaju kada je vjerojatno da će to dovesti do visokog rizika za prava i slobode pojedinaca. Ovaj rizik postoji kada povreda može dovesti do fizičke, materijalne ili nematerijalne štete za pojedince čiji su podaci povrijeđeni.

Primjeri:

Primjeri takve štete su diskriminacija, krađa identiteta ili prijevara, financijski gubitak i narušavanje reputacije. Kada povreda uključuje osobne podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, ili članstvo u sindikatu, ili uključuje genetske podatke, podatke koji se tiču zdravlja ili spolnog života, ili kaznenih osuda i kažnjivih djela ili povezane mjere sigurnosti na, treba smatrati da se takve štete vjerojatno mogu dogoditi.

Čimbenici koje treba razmotriti kod procjene rizika

Uvodne odredbe 75 i 76 GDPR-a sugeriraju da općenito prilikom procjenjivanja rizika, treba uzeti u obzir i vjerojatnost i težinu rizika za prava i slobode ispitanika. Nadalje navodi da rizik treba procijeniti na temelju objektivne procjene.

Treba zapamtiti da procjenjivanje rizika za ljudska prava i slobode kao rezultat povrede ima drugačiji fokus za rizik razmotren kod nekog PUZP-a). PUZP razmatra i rizike obrade podataka koji se provode prema planu, kao i rizike u slučaju povrede. Kod razmatranja potencijalne povrede, gleda se u općenitom smislu na vjerojatnost da se to dogodi, kao i na štetu za ispitanika koja bi iz toga mogla proisteći; drugim riječima, to je procjena hipotetskog događaja. Kod stvarne povrede, događaj se već dogodio, tako da je fokus u cjelini na nastalom riziku učinka povrede na pojedince.

Primjer:

PUZP sugerira da predloženo korištenje posebnog sigurnosnog softverskog proizvoda za zaštitu osobnih podataka je prikladna mjera za osiguravanje razine sigurnosti koja je odgovarajuća riziku koji bi obrada inače predstavljala za pojedince. Međutim, ako ranjivost postane naknadno poznata, to bi promijenilo prikladnost softvera za obuzdavanje rizika za zaštićene osobne podatke i stoga bi se trebao ponovo procijeniti kao dio kontinuiranog PUZP-a.

Ranjivost kod proizvoda se kasnije iskorištava pa dolazi do povrede. Voditelj obrade bi trebao procijeniti specifične okolnosti povrede, pogođene podatke i potencijalnu razinu učinka na pojedince, kao i to koliko je vjerojatno da će se taj rizik doista i ostvariti.

Shodno tome, prilikom procjene rizika za pojedince kao rezultat povrede, voditelj obrade bi trebao razmotriti specifične okolnosti povrede, uključujući težinu potencijalnog učinka i vjerojatnost da se to dogodi. RS29 stoga preporučuje da procjena treba uzeti u obzir sljedeće kriterije:[417]

Vrsta povrede

Vrsta povrede koja se dogodila može imati učinka na razinu rizika nastalog za pojedince.

417 Članak 3.2 Uredbe 611/2013 pruža smjernice o čimbenicima koji bi se trebali uzeti u obzir u odnosu na obavijest o povredama u sektoru usluga elektroničkih komunikacija, što može biti korisno u kontekstu obavještavanja prema GDPR-u. Vidi: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Primjer:

Povreda povjerljivosti, čime se medicinske informacije otkrivaju neovlaštenim osobama, mogu imati drugačiji sklop posljedica za pojedinca od povrede gdje se medicinski podaci o pojedincu izgube pa više nisu dostupni.

Priroda, osjetljivost i obujam osobnih podataka

Naravno da, kod procjene rizika, ključni čimbenik je vrsta i osjetljivost osobnih podataka koji su kompromitirani povredom. Obično, što su podaci osjetljiviji, to je viši rizik štete za pogođene ljude, ali također treba uzeti u obzir i druge osobne podatke koji mogu već biti dostupni o tom ispitaniku. Primjerice, otkrivanje imena i adrese pojedinca u uobičajenim okolnostima vjerojatno neće izazvati značajnu štetu. Međutim, ako se otkrije ime i adresa roditelja usvojitelja biološkom roditelju, posljedice mogu biti vrlo teške i za usvojitelje i za dijete.

Povrede koje uključuju zdravstvene podatke, identifikacijske dokumente ili financijske podatke kao što su podaci s kreditne kartice, mogu izazvati štetu sami po sebi, ali ako se koriste zajedno, oni se mogu koristiti za krađu identiteta. Kombinacija osobnih podataka je u pravilu osjetljivija negoli pojedinačan osobni podatak.

Neke vrste osobnih podataka mogu se na početku činiti relativno bezopasnima, međutim, treba pažljivo razmotriti što ti podaci otkrivaju o pogođenom pojedincu. Popis klijenata koji primaju redovite dostave ne mora biti naročito osjetljiv, ali neki podaci o klijentima koji su zatražili da se njihove isporuke stopiraju za vrijeme godišnjeg odmora bi bili korisne informacije za kriminalce.

Slično tome, malena količina osjetljivih podataka može imati velik učinak na pojedinca, a velik raspon pojedinosti može otkriti veći raspon informacija o tom pojedincu. Također, povreda koja pogađa veliku količinu osobnih podataka o mnogim ispitanicima može imati učinka na odgovarajuće velik broj pojedinaca.

Lakoća identifikacije pojedinaca

Važan čimbenik za razmatranje je koliko će biti lako za osobu koja pristupi kompromitiranim osobnim podacima identificirati pojedine osobe, ili upariti podatke s drugim informacijama kako bi se identificirali pojedinci. Ovisno o okolnostima, identifikacija bi mogla biti moguća izravno iz osobnih podatka na kojima je počinjena povreda bez potrebe za dodatnim istraživanjem radi otkrivanja identiteta pojedinca, ali bi i dalje moglo biti moguće pod određenim uvjetima. Identifikacija može biti izravno ili neizravno moguća iz podataka na kojima je počinjena povreda, ali može također ovisiti o specifičnom kontekstu povrede i javnoj dostupnosti povezanih osobnih pojedinosti. Ovo može biti više relevantno za povjerljivost i povrede dostupnosti.

Kako je prethodno navedeno, osobni podaci zaštićeni odgovarajućom razinom enkripcije bit će neprepoznatljivi neovlaštenim osobama bez ključa za dešifriranje. Osim toga, pravilno provedena pseudonimizacija (definirana u članku 4(5) kao "obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi") može također umanjiti vjerojatnost da se pojedince identificira u slučaju povrede. Međutim, ne može se smatrati da tehnike pseudonimizacije same po sebi čine podatke data neprepoznatljivima.

Težina posljedica za pojedince

Ovisno o prirodi osobnih podataka uključenih u povredu, primjerice, posebne kategorije podataka, potencijalna šteta za pojedince koja može rezultirati iz toga može biti naročito teška, posebice kada bi

povreda mogla dovesti do krađe identiteta ili prijevare, fizičkog ozljeđivanja, psihološke uznemirenosti, poniženja ili narušavanja reputacije. Ako se povreda tiče osobnih podataka o osjetljivim pojedincima, oni mogu biti stavljeni pod veći rizik štete.

Je li voditelj obrade svjestan da su osobni podaci u rukama osoba čije su namjere nepoznate ili moguće zlonamjerne, može imati težinu za razinu potencijalnog rizika. Može doći do povrede povjerljivosti, čime se osobni podaci otkrivaju trećoj strani, kako je definirano u članku 4(10), ili drugom primatelju zabunom. Ovo se može dogoditi, primjerice, kada se osobni podaci pošalju slučajno u pogrešan odjel neke organizacije, ili učestalo korištenu organizaciju dobavljača. Voditelj obrade može zatražiti primatelja ili da vrati ili da sigurno uništi podatke koje je ovaj dobio. U oba slučaja, s obzirom da voditelj obrade ima trajan odnos s tom stranom, te može poznavati njihove procedure, povijest i druge relevantne pojedinosti, primatelj se može smatrati "osobom od povjerenja". Drugim riječima, voditelj obrade može imati stupanj sigurnosti s primateljem tako da može razumno očekivati da ta strana neće pročitati ili pristupiti podacima poslanima zabunom te da će poštivati upute o vraćanju istih. Čak i ako se podacima pristupilo, voditelj obrade bi i dalje moguće vjerovao primatelju da neće poduzeti nikakve daljnje radnje s time i da će vratiti podatke voditelju obrade brzo te surađivati kod vraćanja podataka. U takvim slučajevima, to se može uračunati u procjenu rizika koju voditelj obrade provodi nakon povrede – činjenica da je primatelj osoba od povjerenja može ukloniti težinu posljedica povrede, ali to ne znači i dalje da se povreda nije dogodila. Međutim, to može s druge strane ukloniti vjerojatnost rizika za pojedince, čime se više ne traži obavještavanje nadzornog tijela ili ugroženih pojedinaca. Opet, to će se razlikovati od slučaja do slučaja. Neovisno o tome, voditelj obrade i dalje mora čuvati informacije koje se tiču povrede kao dio svoje opće obveze vođenja evidencije o povredama (…).

Također treba uzeti u obzir trajnost posljedica za pojedince, gdje se učinak može sagledati kao veći ako su učinci dugotrajni.

Posebne karakteristike pojedinca

Povreda može utjecati na osobne podatke koji se tiču djece ili drugih osjetljivih pojedinaca, koji mogu biti suočeni s većim rizikom opasnosti kao rezultat toga. Mogu postojati i drugi čimbenici o pojedincu koji mogu utjecati na razinu učinka povrede na njih.

Posebne karakteristike voditelja obrade

Priroda i uloga voditelja obrade i njihovih aktivnosti može utjecati na razinu rizika za pojedince kao rezultat povrede. Primjerice, ustanova koja pruža medicinske usluge će obrađivati posebne kategorije osobnih podataka, što znači da postoji veća prijetnja za pojedince ako dođe do povrede njihovih osobnih podataka, u usporedbi s popisom adresa pojedinaca kod dostave novina.

Broj ugroženih pojedinaca

Povreda može utjecati samo na jednog ili nekolicinu pojedinaca ili pak stotine tisuća, ako ne i više. Općenito, što je veći broj pojedinaca pogođen, to veći učinak povreda može imati. Međutim, povreda može imati značajan učinak na čak jednog pojedinca, ovisno o prirodi osobnih podataka i kontekstu u kojem su isti kompromitirani. Opet, ključno je razmotriti vjerojatnost i težinu učinka na one koji su pogođeni.

Opći naglasci

Stoga, kod procjene rizika koji vjerojatno proizlazi iz povrede, voditelj obrade bi trebao razmotriti kombinaciju težine potencijalnog učinka na prava i slobode pojedinaca i vjerojatnost da se isti pojavi. Očigledno, kada su posljedice povrede teže, rizik je veći, a slično tome, kad je vjerojatnost da se to dogodi veća, onda se i rizik povećava. Ako postoji sumnja, voditelj obrade bi se trebao prikloniti pristupu opreznosti i obavijestiti. Prilog B daje neke korisne primjere različitih vrsta povreda koje uključuju rizik ili visoki rizik za pojedince.

Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) je izradila preporuke za metodologiju procjene težine povrede, koja može biti korisna voditeljima i izvršiteljima obrade kod izrade svojeg plana za odgovor na upravljanje povredom.[418]

Prilog:

Primjeri povreda osobnih podataka i koga treba obavijestiti (iz RS29 Smjernica)

	Primjer	Obavještavanje nadzornog tijela?	Obavještavanje ispitanika?	Bilješke/ preporuke
i.	Voditelj obrade je pohranio sigurnosnu kopiju (*backup*) arhive enkriptiranih osobnih podataka na USB ključu. Ključ je ukraden tijekom provale.	Ne.	Ne.	Dokle god su podaci enkriptirani vrhunskim algoritmom, sigurnosne kopije postoje, jedinstveni ključ nije kompromitiran, i podaci se mogu u razumno vrijeme vratiti, to moguće nije povreda koju treba prijaviti. Međutim, ako kasnije budu kompromitirani, potrebno je obavještavanje.
ii.	Voditelj obrade ima mrežnu uslugu. Kao rezultat kibernetičkog napada na tu uslugu, izvučeni su osobni podaci pojedinaca. Voditelj obrade ima klijente u samo jednoj državi članici.	Da, obavijestite nadzorno tijelo ako postoje vjerojatne posljedice za pojedince.	Da, obavijestite pojedince ovisno o prirodi ugroženih osobnih podataka, te ako je težina vjerojatnih posljedica za pojedince visoka.	
iii.	Kratak nestanak struje u trajanju od nekoliko minuta u pozivnom centru voditelja obrade, što znači da kupci ne mogu zvati voditelja obrade i pristupiti svojim evidencijama	Ne.	Ne.	Ovo nije povreda koju treba prijaviti, ali i dalje jest incident kojeg treba zabilježiti po članku 33(5). Odgovarajuće evidencije treba održavati voditelj obrade.
iv.	Voditelj obrade pretrpi napad ucjenjivačkim softverom (*ransomware*), što dovodi do toga da su svi podaci enkriptirani. Nikakve sigurnosne kopije nisu dostupne i podaci se ne mogu vratiti. Nakon istrage, postaje jasno da je jedina funkcionalnost malicioznog softvera bila enkriptirati podatke, te da nije bilo drugog *malwarea* u sustavu.	Da, obavijestite nadzorno tijelo, ako postoje vjerojatne posljedice za pojedince jer ovo jest gubitak dostupnosti.	Da, obavijestite pojedince, ovisno o prirodi ugroženih osobnih podataka i mogućem učinku manjka dostupnosti podataka, kao i njihovim vjerojatnim posljedicama.	Ako su bile dostupne sigurnosne kopije (*backup*) i podaci se mogu vratiti u skorije vrijeme, to ne bi trebalo prijaviti nadzornom tijelu ili pojedincima jer ne bi bilo trajnog gubitka dostupnosti ili povjerljivosti. Međutim, ako je nadzorno tijelo saznalo za incident drugim putem, može razmotriti istragu da bi provjerilo sukladnost sa širim zahtjevima za sigurnost iz članka 32.

418 ENISA, Preporuke za metodologiju procjene težine povreda osobnih podataka, https://www.enisa.europa.eu/publications/dbn-severity

v.	Osoba telefonom zove pozivni centar banke da bi prijavila povredu podataka. Pojedinac je zaprimio mjesečni izvještaj za nekoga drugoga. Voditelj obrade poduzima kratku istragu (tj. završenu unutar 24 sata) i ustanovljuje s razumnom sigurnošću da se povreda osobnih podataka dogodila i ima li sistemsku grešku koja može značiti da su i drugi pojedinci bili ili bi mogli biti ugroženi.	Da.	Obavještava se samo ugrožene pojedince ako postoji visok rizik i jasno je da drugi nisu bili ugroženi.	Ako, nakon daljnje istrage, bude prepoznato da je ugroženo više pojedinaca, moraju se poslati ažurirane informacije nadzornom tijelu, a voditelj obrade poduzima dodatne korake obavještavanja drugih pojedinaca ako za njih postoji visok rizik.
vi.	Voditelj obrade vodi mrežnu trgovinu i ima klijente u više država članica. Trgovina pretrpi kibernetički napad tako da napadač objavi korisnička imena, lozinke i povijest kupnji na mreži.	Da, obavijestite vodeće nadzorno tijelo ako to uključuje prekograničnu obradu.	Da, jer bi moglo dovesti do visokog rizika.	Voditelj obrade bi trebao poduzeti radnje, tj. forsirajući ponovno postavljanje lozinki za ugrožene račune, kao i druge mjere za ublažavanje rizika. Voditelj obrade bi također trebao razmotriti bilo koje druge obveze obavješćivanja, npr. sukladno NIS Direktivi kao pružatelj digitalnih usluga.
vii.	Društvo koje pruža usluge hostinga mrežnih stranica, koje djeluje kao izvršitelj obrade, identificira grešku u kodu koji kontrolira autorizaciju korisnika. Učinak greške znači da bilo koji korisnik može pristupiti podacima o računu bilo kojeg drugog korisnika.	Kao izvršitelj obrade, društvo koje pruža usluge hostinga mrežnih stranica mora obavijestiti svoje ugrožene klijente (voditelje obrade) bez nepotrebnog odugovlačenja. Pretpostavljajući da je društvo za usluge hostinga mrežnih stranica provelo svoju vlastitu istragu, ugroženi voditelji obrade bi razumno trebali imati povjerenja o tome je li svaki od njih pretrpio povredu i stoga je vjerojatno smatrati da je "saznao" kad ih je obavijestilo društvo koje pruža usluge hostinga (izvršitelj obrade). Voditelj obrade mora tada obavijestiti nadzorno tijelo.	Ako nije vjerojatno da će nastupiti visok rizik za pojedince, oni ne trebaju biti obaviješteni.	Društvo koje pruža usluge hostinga (izvršitelj obrade) mora razmotriti bilo koje druge obveze obavješćivanja (npr. sukladno NIS Direktivi kao pružatelj digitalnih usluga). Ako nema dokaza da je ova ranjivost iskorištena kod bilo kojeg od njegovih voditelja obrade, značajna povreda se možebitno nije dogodila, ali je vjerojatno da je treba evidentirati ili da bude predmet nesukladnosti prema članku 32.
viii.	Zdravstvene evidencije u bolnici su nedostupne u trajanju od 30 sati zbog kibernetičkog napada.	Da, bolnica je dužna obavijestiti o tome jer se visok rizik za dobrobit i privatnost pacijenata može dogoditi.	Da, obavijestite pogođene pojedince.	
ix.	ix. Osobni podaci velikog broja studenata su pogreškom poslani na pogrešan popis e-adresa s 1000+ primatelja.	Da, obavijestite nadzorno tijelo.	Da, obavijestite pojedince, ovisno o broju i vrsti osobnih podataka koji su uključeni, te o težini mogućih posljedica.	

x.	x. E-poruka sadržaja izravnog marketinga je poslana primateljima pod "to:" ili "cc:" poljima, time omogućujući primatelju da vidi adrese e-pošte drugih primatelja.	Da, obavještavanje nadzornog tijela može biti obvezno ako je pogođen velik broj pojedinaca, ako su otkriveni osjetljivi podaci, (npr. adresar psihoterapeuta s adresama e-pošte klijenata) ili ako drugi čimbenici predstavljaju visoke rizike (npr. e-pošta sadrži početne lozinke).	Da, obavijestite pojedince ovisno o broju i vrsti uključenih osobnih podataka i težini mogućih posljedica.	Obavijest ne mora biti nužna ako nisu otkriveni nikakvi osjetljivi podaci i ako je otkriven samo manji broj adresa e-pošte.

7. ZADAĆA: Istražna zadaća (uključujući rješavanje i internih i eksternih pritužbi)

Bilješka: Ova je zadaća odvojena i različita od rješavanja zahtjeva ispitanika za pristup, ispravak itd., o čemu se govori u 8. zadaći.

ISTRAGA

Iako ovo nije izrijekom spomenuto u GDPR-u, slijedi iz širokog opisa cjelokupnog položaja i zadaća SZP-a – a posebice iz obveze SZP-a "praćenje sukladnosti" s GDPR-om: čl. 39(1)(b) – da SZP može, na vlastitu inicijativu ili na zahtjev uprave ili, npr. predstavničkog tijela zaposlenika ili sindikata ili doista bilo kojeg pojedinca (iz organizacije ili bez organizacije, ili čak zviždača, koji je, nadajmo se, zaštićen u dotičnoj državi) **istražiti** pitanja i događaje koji su izravno vezani za zadaće SZP-a i povratno **izvijestiti** osobu ili tijelo koje je naručilo ili zatražilo istragu i/ili vrhu uprave. Kako ENZP navodi u svojem Radu o stajalištu na temu SZP-ova:[419]

> **Praćenje sukladnosti** (…): SZP treba osigurati primjenu Uredbe unutar institucije. SZP može, na vlastitu inicijativu ili na zahtjev institucije ili tijela, voditelja obrade, radničkog vijeća ili bilo kojeg pojedinca istraživati predmete i događaje koji su izravno vezani za zadaće SZP-a i povratno izvijestiti osobu koja je naručila istragu ili voditelja obrade.

GDPR jasno kaže – premda koristeći manje izričit rječnik negoli u Prilogu uz uredbu o zaštiti podataka u EU institucijama – da se SZP-ovima mora dati **sve relevantne resurse** i **pristup svim podacima i prostorijama, instalacijama za obradu podataka i medijima za prijenos podataka** (sa svim relevantnim i potrebnim ***odobrenjima*** i ovlastima ***pristupa i zadržavanja elektroničkih zapisa***) koji su nužni za provođenje zadaća SZP-a (usp. čl. 38(2)), tj. također u odnosu na takve istrage.[420] Slično tome, iako je ovo opet izrijekom navedeno u odnosu na SZP-ove europskih institucija negoli za SZP-ove prema GDPR-u, **svi zaposlenici dotičnog voditelja obrade – a zapravo i bilo koje osoblje vanjskih agencija, uključujući posebice određene izvršitelje obrade (uključujući pružatelja usluga u oblaku, koje koristi voditelj obrade) – trebaju u cijelosti pomoći SZP-u kod bilo kojih takvih istraga,** i davati ***cjelovite odgovore i informacije*** na bilo koja pitanja ili zahtjeve koje postavi SZP.[421] **Voditelji obrade bi trebali ovo učiniti eksplicitno jasnim u internim smjernicama za zaposlenike te trebaju uključiti jasne odredbe u tom smislu u njihove ugovore s vanjskim pružateljima usluga i izvršiteljima.**

419 EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (bilješka 243, iznad), str. 6, izvorni naglasak podebljanim slovima.
420 *Prilog* uz Uredbu (EU) 45/2001 navodi SZP-ovi EU institucija: "će imati pristup u svako doba podacima koji predstavljaju predmet postupaka obrade i svim uredima, instalacijama za obradu podatka i nosačima podatka". (*Prilog*, članak 4, druga rečenica).
421 *Prilog* uz Uredbu (EU) 45/2001 propisuje da: "*Svaki voditelj obrade će trebati pomoći Službeniku za zaštitu podataka u obavljanju njegovih/njenih obveza i dati informacije kao odgovor na sva pitanja*." (*Prilog*, čl. 4, prva rečenica).

PROVEDBA

Usprkos tome što je nadležan za praćenje sukladnosti s GDPR-om, rješavati pritužbe i istraživati moguće povrede Uredbe, SZP **ima ograničene ovlasti provedbe.** U načelu, kako je opisano, ako SZP zaključi da se u nekom smislu nije poštivalo GDPR u njegovoj organizaciji, ili od strane bilo kojeg vanjskog pružatelja usluga ili izvršitelja, SZP bi to trebao prijaviti višoj razini uprave – a tada je odgovornost uprave da poduzme korektivne mjere, uključujući, kada je to prikladno, sankcije protiv bilo kojeg zaposlenika ili agenata ili izvršitelja koji su propustili izvršiti svoje odnosne obveze, npr. izdavanjem upozorenja ili drugih kazni ili, u ekstremnim slučajevima, otkaz ili prekid ugovora. Primjerice, ako se koristi vanjski pružatelj usluga za prikupljanje podataka (npr. putem automatiziranog sustava kojim upravlja pružatelj usluge), a taj pružatelj usluge ne poštuje GDPR, npr. u smislu obavještavanja ili, još gore, koristeći prikupljene podatke potajno za daljnje (neprijavljene) svrhe, SZP treba predložiti da voditelj obrade koristi drugog pružatelja usluge, te u isto vrijeme alarmirati TZP.

Propust poduzeti takve radnje, uzet će se na štetu voditelja obrade (organizacije) kod razmatranja radnje provedbe od strane nadzornog tijela za zaštitu podataka (TZP), uključujući kod postavljanja granice bilo koje "upravno novčane kazne" koja može biti nametnuta (usp. čl. 83).

Štoviše, jedna od zadaća SZP-a je "savjetovati" relevantni TZP, "prema potrebi", u pogledu bilo kojeg pitanja koje se javi (čl. 39(1)(e)). U slučaju ozbiljne razlike stajališta između SZP-a i najviše razine uprave njegove/njene organizacije, kada, po mišljenju SZP-a, određeni postupak obrade predstavlja ili će predstavljati (ozbiljnu) povredu GDPR-a, i/ili relevantnog nacionalnog zakona, ali ga uprava i dalje želi poduzeti, ili pak protiv čega nema namjeru izreći nikakve sankcije, svakako bi se činilo da je "prikladno" da SZP ostvari ovu ovlast i (učinkovito) proslijedi predmet TZP-u. Tada će biti na TZP-u da iskoristi svoje – snažne – istražne i provedbene ovlasti, uključujući mogućnost narediti neprovedbu ili zaustavljanje obrade, kako samo tijelo (TZP) smatra prikladnim (vidi čl. 58(2)(d) i (f) naročito).

Vidi dalje u nastavku, pod naslovima "*Suradnja s i savjetovanje s TZP-om*" i "*Rješavanje upita i pritužbi*".

SAVJETODAVNE ZADAĆE

8. ZADAĆA: Savjetodavna zadaća – općenito

SZP-ovi moraju osigurati da se Uredba poštuje i savjetovati voditelje obrade o ispunjavanju njihovih obveza. SZP može stoga **informirati**, pružati **savjete** ili davati **preporuke** za ***praktično poboljšanje*** zaštite podataka od strane organizacije i/ili o pitanjima koja se tiču primjene odredbi o zaštiti podataka (tj. GDPR-a i drugih zakona o EU zaštiti podataka – kao što su, za sada, Direktiva o e-privatnosti iz 2002. i, u budućnosti, moguća Uredba o e-privatnosti – kao i bilo kojeg nacionalnog zakona koji proširuje posebne klauzule iz GDPR-a ili kako je na drugi način primjenjivo); i za ***izmjene i ažuriranja politika (pravila) i praksi organizacije vezano za zaštitu podataka*** u svjetlu novih pravnih instrumenata, odluka, mjera ili smjernica (usp. čl. 39(1)(a)).

Radi toga, SZP bi trebao moći **pažljivo pratiti zakonodavstvo i regulatorna događanja u područjima zaštite podataka, sigurnosti podataka itd.**, kako bi mogao alarmirati višu razinu uprave i odgovarajuću nižu razinu uprave o nadolazećim ***novim EU instrumentima*** (kao što je Uredba o e-privatnosti, upravo spomenuta) ili nove ***izvršne ili sudske odluke na EU-razini*** (kao bilo koja relevantna odluka o "primjerenosti" Europske komisije, koja se odnosi na treće zemlje u koje organizacija SZP-a prenosi podatke, ili relevantne presude SEU-a); ***nove smjernice na EU razini*** (posebice, bilo koja mišljenja ili preporuke, itd. koje izda ***EOZP***); i ***slični instrumenti, odluke, mjere ili smjernice koje su izdane u vlastitoj državi*** poslovnog nastana ***SZP-a*** (ili državama). GDPR doista **zahtijeva** od svakog voditelja obrade sa SZP-om da pruži SZP-u "***[sva] potrebna sredstva*** *za izvršavanje [svojih] zadaća … i* ***za održavanje njegova [njenog] stručnog znanja***" (čl. 38(2)). SZP-u se stoga treba dopustiti – i doista ga poticati – da pohađa relevantne seminare, konferencije i sastanke, posebice one koje god organizira(ju) nacionalno ili regionalno tijelo(a) za zaštitu podataka.

I uprava **također može tražiti od** SZP-a **savjet**, kao i radničko vijeće ili sindikat, ili čak bilo koji zaposlenik, uključujući naravno bilo kojeg "vlasnika posla"/osobe unutar organizacije sa specifičnim odgovornostima za specifične postupke obrade, kada god takva osoba želi dobiti savjet – i doista općenito **mora** ga se pitati za savjet o relevantnim pitanjima (usp. također 7. zadaću, koja je sljedeća tema).

Kako je RS29 naveo u svojim Smjernicama o SZP-ovima (od kad ih je formalno podržao EOZP):[422]

Posljedično, organizacija bi trebala osigurati, primjerice, da:

- SZP bude pozvan sudjelovati redovito na sastancima višeg i srednjeg menadžmenta.
- Njegova/njena nazočnost se preporučuju kad se donose odluke s implikacijama za zaštitu podataka. Sve relevantne informacije se moraju prenijeti SZP-u pravovremeno kako bi mu/joj se omogućilo da pruži adekvatan savjet.
- Mišljenju SZP-a se uvijek mora dati težina. U slučaju neslaganja, RS29 preporučuje, kao dobru praksu, dokumentirati razloge zbog propusta postupanja po savjetu SZP-a.
- Od SZP-a se mora hitno tražiti savjet kada se pojavi povreda podataka ili drugi incident.

Kada je prikladno, voditelj ili izvršitelj obrade bi mogli izraditi smjernice za zaštitu podataka ili programe koji popisuju kada se SZP-a mora tražiti za savjet.

422 RS29, Smjernice o SZP-ovima (bilješka 242, prethodno u tekstu), str. 13-14.

9. ZADAĆA: Podržavanje i promoviranje "Tehničke i integrirane zaštite podataka"

Kako je navedeno u tekstu kod 6. zadaće, SZP se općenito mora tražiti savjet o pitanjima koja se odnose na zaštitu podataka koja se javljaju unutar organizacije SZP-a, uključujući u to i sastavljanje smjernica o glavnim politikama (pravila) itd.

Međutim, postoji jedna stvar koja je od posebne važnosti u ovom smislu. To je novi izričiti zahtjev iz GDPR-a (koji još nije bio izrečen u Direktivi o zaštiti podataka iz 1995. g., premda ga se moglo, i može se, iščitati u tome),[423] da voditelji podataka usvoje načelo "**tehnička i integrirana zaštita podataka**" (što uključuje načelo "***tehničku zaštitu [i integriranu]***")[424] u svim svojim obradama. Kako je napisano u članku 25:

> Članak 25.
>
> **Tehnička i integrirana zaštita podataka**
>
> 1. Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.
> 2. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.
> 3. … [425]

Mi možemo samo kratko raspraviti o načelo iznesenom ovdje. ENZP sumira **opći koncept i njegovu pozadinu** kako slijedi:[426]

Izraz "*privacy by design*" izvorno je koristila Ann Cavoukian kad je radila kao Povjerenica za informacije i privatnost u gradu Ontario, Kanada. U njenom konceptu, tehnička zaštita podataka može se rastaviti na "**7 temeljnih načela**",[427] naglašavajući potrebu biti **proaktivan** kod razmatranja zahtjeva privatnosti [ili terminologijom EU-a: zaštita podataka] kao faze izrade širom cjelovitog životnog ciklusa podataka, biti "*ugrađen u dizajn i arhitekturu IT sustava i poslovnih praksi ...ne umanjujući time funkcionalnost...*", uz zaštitu podataka kao zadane postavke, sveobuhvatnu sigurnost, uključujući sigurno uništenje podataka i snažnu transparentnost podložnu neovisnoj verifikaciji. Načelo tehničke zaštite podataka bilo je potaknuto kao drugo od temeljnih načela, ustanovljavajući da tehnička zaštita podataka uključuje "*osiguravanje da su osobni podaci automatski zaštićeni u bilo kojem zamislivom IT sustavu ili poslovnoj praksi. Ako pojedinac ne čini ništa, njihova privatnost i dalje ostaje netaknuta. Nikakva aktivnost se ne traži na strani pojedinca radi zaštite njihove privatnosti — **to je ugrađeno u sustav, zadano je***". Ova izjava je snažna operativna definicija načela

423 Usp., primjerice, ponovljenu referencu na načelo u RS29 Mišljenje 8/2014 on the on Recent Developments on the Internet of Things (WP223), usvojeno 16. rujna 2014, dostupno na: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

424 Usp. RS223 (prethodna bilješka), p. 22, pretposljednja točka.

425 Treći stavak navodi da: "*Odobreni mehanizam certifikacije sukladno članku 42. može se koristiti kao element dokazivanje sukladnosti sa zahtjevima iznesenima u stavcima 1 i 2 ovog članka.*" O ovome se raspravlja u odnosu na 8. zadaću, dalje u tekstu.

426 ENZP, Preliminary Opinion on privacy by design (Opinion 5/2018), issued on 31 May 2018, p. 4, para. 17 (original italics),available at: https://ENZP.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (dodan naglasak)
Primijetite da ENZP razlikuje šire načelo "privacy by design", koje ima "vizionarsku i etičku dimenziju", od specifičnijih zakonskih zahtjeva "tehničke zaštite podataka" i "integrirane zaštite podataka" iz članka 25 GDPR-a: str. 1, st. 4.

427 Vidi: "Sedam temeljnih načela" su: 1. Proaktivan, a ne reaktivan, Preventivan, a ne remedijski; 2. Privatnost kao zadana postavka; Privatnost uklopljena u dizajn; 4. Potpuna funkcionalnost – Pozitivan zbroj, Zbroj nije nula; 5. Sigurnost s-kraja-na-kraj – Zaštita tijekom čitavog životnog vijeka; 6. Vidljivost i transparentnost – ostavite otvoreno; 7. Poštivanje korisničke privatnosti – Neka korisnik bude u središtu [original bilješka]. https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

tehničke zaštite privatnosti, gdje pojedinac ne snosi teret težnje za zaštitom prilikom korištenja usluge ili proizvoda, već uživa "automatski" (bez potrebe za aktivnim ponašanjem) temeljno pravo na privatnost i zaštitu osobnih podataka.

Po mišljenju ENZP, "tehnička zaštita podataka" ima **nekoliko dimenzija**; da parafraziramo:[428]

- **prva je dimenzija** da postupci obrade osobnih podataka trebaju uvijek biti ***ishod dizajna projekta***, obuhvaćajući ***cjelovit životni ciklus projekta***, unutar kojega rizici i zahtjevi zaštite podataka trebaju biti jasno identificirani;
- **druga je dimenzija** da se dizajn projekta treba zasnivati na ***pristupu upravljanja rizikom***, unutar kojeg resursi koji trebaju biti zaštićeni jesu ***pojedinci čiji se podaci trebaju obraditi, a posebice njihova temeljna prava i slobode***;
- **treća dimenzija** je da mjere poduzete za zaštitu tih pojedinaca i prava i sloboda moraju biti ***prikladne i učinkovite*** u odnosu na te rizike, gledano u svjetlu načela zaštite podataka iznesenih u članku 5. GDPR-a, što se može sagledati kao ***ciljevi koje treba postići***;
- četvrta dimenzija je obveza ***integrirati identificirane [nužne, prikladne i učinkovite] zaštitne mjere u obradu podataka***.

Još dodaje da:[429] **Sve su četiri dimenzije jednako važne i postaju sastavni dio pouzdanosti [odgovornosti]** te podliježu nadzoru od strane nadležnog nadzornog tijela, kada je to prikladno. ENZP naglašava važnost tehničke i integrirane zaštite podataka u odnosu na različite uloge: voditelji obrade i izvršitelji općenito;[430] razvojni inženjeri (osjetljivi na pitanja privatnosti) proizvoda i tehnologija;[431] usluge e-komunikacija;[432] usluge e-identiteta;[433] pružatelji "smart" mreža.[434] U odnosu na **javnu upravu**, ENZP naglašava da:[435]

> Članak 25. se primjenjuje na sve vrste organizacija koje djeluju kao voditelji obrade, uključujući **javnu upravu**, koja bi, uzevši u obzir njihovu ulogu da služe općem dobru, **trebala dati primjer kod zaštite temeljnih prava i sloboda pojedinca**. GDPR naglašava ulogu tehničke i integrirane zaštite podatka kada javna uprava treba identificirati dobavljače proizvoda i pružatelje usluga u Uvodnoj odredbi 78, navodeći sljedeće ***"Načela tehničke i integrirane zaštite podataka bi također trebalo uzeti u obzir u kontekstu javnih natječaja."*** **Javnu upravu se poziva da bude u prvom redu kod primjene tih načela na odgovoran način, spremna dokazati njenu primjenu**, ako je potrebno, nadležnom nadzornom tijelu…

Spominjanje **javnih natječaja** je posebno važno: SZP-ovi bi trebali pružati savjet svojoj organizaciji da prilikom izdavanja takvih natječaja, javna bi uprava trebala izrijekom objaviti natječaj za podnositelje koji mogu "dokazati" da je njihov proizvod ili usluga u cijelosti sukladan/na s GDPR-om (i drugim relevantnim EU i nacionalnim zakonima za zaštitu podatka),[436] te da su ugradili "tehničku i integriranu zaštitu osobnih podatka" u relevantan proizvod ili uslugu. Trebalo bi doista biti moguće dati ***kompetitivnu prednost*** takvim podnositeljima ispred i prije drugih čiji proizvodi ili usluge za koje se ne može dokazati da udovoljavaju tim zahtjevima.[437]

ENZP raspravlja donekle detaljno o različitim **metodologijama** koje su razvijene radi primjene tehničke i integrirane zaštite podataka.[438] Ovo se ne može objašnjavati u ovom radu u cijelosti niti čak parafrazirano – ali SZP-ovi bi se trebali u cijelosti upoznati s time (doista, detaljnije negoli je izneseno u radu ENZP-a). Dostatno je primijetiti da **ENZP s pravom povezuje tehničku i integriranu zaštitu podataka s procjenom učinka na**

428 Za potpune detalje o tim dimenzijama kako ih vidi ENZP, vidi Preliminarno mišljenje 5/2018 (bilješka 437, iznad), str. 6-7 (st. 27 – 32).
429 *Idem*, p. 7, para. 32, dodan naglasan podebljanim slovima.
430 *Idem*, p. 7, st. 35 – 36.
431 *Idem*, str. 7, st. 37.
432 *Idem*, str. 8-9, st. 42 – 44 (s referencom na Direktivu o e-privatnosti i predloženu Uredbu o e-privatnosti).
433 *Idem*, str. 9, para. 45 (s referencom na eIDAS Uredbu).
434 *Idem*, str. 9- 10, st. 46 – 50 (s referencom na Smart Meter DPIA Template preporuku).
435 *Idem*, str. 8, para. 38, izvornik u kurzivu (*italic*), naglasak debelim slovima dodan.
436 Vidi raspravu o načelu "pouzdanosti" ["odgovornosti"] u Drugom dijelu, odlomak 2.4, iznad.
437 Ovaj stav je izrijekom usvojen po Schleswig-Holstein zakonu o zaštiti podataka.
ENZP, Preliminarno mišljenje 5/2018 (bilješka 437, iznad), str. 13-15, st. 63 – 72. Vidi također specifične reference na U.S. NIST program za inženjering privatnosti i njegov izvještaj o inženjeringu privatnosti i upravljanju rizikom za američke savezne sustave (str. 11, st. 56, bilješke 76 i 74) i EU ENISA 2014 najmodernija (tada) analiza (str. 12, st. 59, bilješka 82).

zaštitu podatka (PUZP), kako je objašnjeno u 4. zadaći, prethodno u tekstu);[439] a općenitije da, kako ENZP također izrijekom naglašava:[440]

> **Uloga privatnosti i službenika za zaštitu podatka je ključna, a njihovo uključivanje je presudno za pristup tehničkoj zaštiti podataka.** Oni moraju biti u petlji od početnih stadija kada organizacije planiraju sustave za obradu osobnih podataka, tako da mogu podržati direktore, vlasnike posla, te odjele za IT i tehnologiju, prema potrebi. Njihov skup vještina treba odgovarati tim zahtjevima.

Taj "skup vještina" bi trebao uključivati da je osoba **potpuno obrazovana i osposobljena na području relevantnih metodologija** i tehnologija (ako je potrebno, onda i dodatnim osposobljavanjem na radnom mjestu), kao i to da treba biti **duboko uključena u izradu, razvoj, testiranje i podešavanje svih osjetljivih (po pitanju privatnosti) proizvoda, usluga i radnji svoje organizacije** (uključujući javne natječaje, kako je upravo spomenuto), u svim stadijima.

10. ZADAĆA: Savjetovanje o i praćenje sukladnosti s politikama (pravilima) zaštite podatka, ugovori između zajedničkih voditelja obrade, voditelja obrade - voditelja obrade i voditelja obrade - izvršitelja obrade, Obvezujuća korporativna pravila i klauzule o prijenosu podataka

Kako bi se postigla sukladnost s GDPR-om, a posebice se "dokazala" takva sukladnost, voditelji obrade mogu i trebaju usvojiti ili se uključiti u niz mjera. Kako je navedeno pod točkom 2.2.2, prethodno u tekstu, ovo uključuje:

- sastavljanje i formalno usvajanje internih **politika (pravila) zaštite podataka** (vidi čl. 24(2)) da bi se regulirala pitanja, kao što su:
  - **papirnati obrasci organizacije, mrežni obrasci** i **izjave o zaštiti podataka/privatnosti na mrežnim stranicama**, korištenje **kolačića** (*cookies*) i drugog lokacijskog softvera (*trackers*) neke organizacije;
  - **pristupni el. zapisi (logovi) i alternacijski** itd., u relevantnom softveru i hardveru;
  - izdavanje "zakrpa" ("**patches**") za vlastiti softver;
  - itd.
- usvajanje **administrativnih aranžmana** ("**aranžmani**") između javnih tijela vlasti, posebno ako se za njih može reći da su "**zajednički voditelji obrade**" nad određenim postupcima obrade;
- izrada i ugovaranje relevantnih **ugovora s drugim voditeljima obrade i izvršiteljima obrade**; i
- pridruživanje ili standardnih ili ugovornih klauzula **o prijenosu podataka**.

Glavna poanta koju ovdje treba ponovo naglasiti je da su ovo sve odgovornosti (sredstva "dokazivanja sukladnosti") voditelja obrade, a ne SZP-a (vidi pododlomak na temu "*Nepostojanje odgovornosti SZP-a za sukladnost s GDPR-om*", u Drugom dijelu, pod točkom 2.5.4, prethodno u tekstu).

Međutim, u praksi bi SZP opet trebao biti blisko uključen u sve takve predmete. U najmanju ruku, bilo koji novi SZP – a posebno SZP imenovan u organizaciji koja prethodno nije imala SZP-a – bi trebao **preispitati** sve postojeće dokumente i instrumente ove vrste, kako bi provjerio/la ispunjavaju li oni i dalje u cijelosti sve pravne zahtjeve zaštite podataka.

Temeljem takvog preispitivanja, on/a bi trebao/la **preporučiti promjene u postojećim dokumentima itd.** – posebno ako su isti sastavljeni i usvojeni prije usvajanja i stupanja na snagu GDPR-a; i SZP bi trebao/la

439 *Idem*, str. 8, st. 39 – 40.
440 *Idem*, str. 15, para. 76, dodan naglasak.

preporučiti sastavljanje i usvajanje takvih dokumenata itd. u slučajevima kada bi (po mišljenju SZP-a) takvi dokumenti trebali postojati ali ne postoje.

A SZP je formalno zadužen za praćenje sukladnosti sa svim politikama (pravilima), aranžmanima i ugovorima usvojenima ili sklopljenima od strane voditelja obrade u odnosu na obradu osobnih podataka (usp. čl. 39(1)(b)).

11. ZADAĆA: Uključenost u kodekse ponašanja i certifikacije

Napisali smo u Drugom dijelu, pod točkom 2.2.2, prethodno u tekstu, da poštivanje i potpuna sukladnost s odobrenim **kodeksom ponašanja** ili odobrenim mehanizmom **certificiranja zaštite podataka**, bi također mogla služiti kao važno sredstvo za dokazivanje sukladnosti s GDPR-om u odnosu na teme obuhvaćene u takvim kodeksima ili mehanizmima certificiranja.

Opet, na kraju će ostati na voditelju obrade – ne na SZP-u – naime, da odluči slijediti relevantan kodeks ponašanja za sektor u kojem organizacija djeluje, ili pak traži odobrenje mehanizma certificiranja zaštite podataka tipa zamišljenog u Uredbi (vidi čl. 40 – 43). Međutim, bilo bi sasvim prihvatljivo da SZP **predloži** takvo djelovanje.

Doista, moglo bi biti prilično prikladno da SZP-ovi iz organizacija koje rade u određenom sektoru budu uključene u **sastavljanje kodeksa ponašanja** za taj sektor, iako bi to također trebalo uključivati pravnika i osoblje sektorske organizacije pod čijim se krilom kodeks izrađuje (uključujući posebice ICT osoblje ako se kodeks dotiče tehničkih pitanja, kao što su ICT sigurnost, enkripcija itd.).

SZP može također **pomoći kod odobrenja mehanizma certificiranja** za organizaciju SZP-a, i to pomažući kod sastavljanja ili pružanja certifikacijskom tijelu "sve[ih] informacije[a] i pristup svojim aktivnostima obrade koje su potrebne za vođenje postupka certificiranja certifikacijskom tijelu" (čl. 42(6)). Međutim, kada se certifikacijska shema oslanja na **procjenu** postupaka obrade osobnih podataka voditelja obrade od strane jednog ili više **neovisnih stručnjaka** akreditiranog od strane nadležnog Certifikacijskog tijela (kako je napravljeno u glavnoj trenutnoj shemi u EU, *European Privacy Seal [EuroPriSe]* shema),[441] SZP ne može djelovati u toj ulozi: to bi predstavljalo sukob interesa.

Opaska: U nekoj mjeri, detaljne evidencije procjene učinka na zaštitu podataka (PUZP), obrazloženo pod 4. zadaćom, prethodno u tekstu te kontinuirano nadgledanje aktivnosti, kako je razmotreno 5. zadaćom, prethodno u tekstu (i evidencija navedenih kontinuiranih praćenja) ispunjavaju sličnu svrhu kao i certificiranje, u smislu da prikazuje da su voditelj obrade i njegovi zaposlenici pažljivo pregledali sve implikacije privatnosti/zaštite podataka relevantnih postupaka obrade osobnih podatka; identificirali su i kvantificirali uključene rizike za temeljna prava pogođenih pojedinaca; te su usvojili odgovarajuće mjere za ublažavanje rizika. Prednost certifikacije pred time je da evaluaciju rade vanjski, neovisni stručnjaci. Međutim, mnogo će toga ovisiti o kvaliteti akreditiranih certifikacijskih shema te o tome kako će se odnositi prema izvršavanju od strane TZP.

441 Vidi: https://www.european-privacy-seal.eu/EPS-en/fact-sheet

SURADNJA S I SAVJETOVANJE S TZP-OM

12. ZADAĆA: Suradnja s TZP-om

SZP ima zadaću odgovoriti na zahtjeve TZP-a i, unutar sfere svoje kompetencije, surađivati s TZP-om na njegov zahtjev ili na vlastitu inicijativu (čl. 39(1)(d)).

U tom smislu, RS29 navodi:[442]

> Ove se zadaće odnose na ulogu "facilitatora" SZP-a, spomenutog u uvodu ove Smjernice. SZP djeluje kao kontaktna točka kako bi olakšao pristup nadzornog tijela dokumentima i informacijama radi obavljanja zadaća navedenih u članku 57., kao i radi izvršavanja istražnih, korektivnih, ovlasti u vezi s odobravanjem i savjetodavnih ovlasti spomenutih u članku 58. kako je prethodno spomenuto, SZP je obvezan tajnošću ili povjerljivošću u vezi s obavljanjem svojih zadaća, u skladu s pravom Unije ili pravom države članice (članak 38(5)). Međutim obveza tajnosti/povjerljivosti ne zabranjuje SZP-u da kontaktira i zatraži savjet od nadzornog tijela. Članak 39(1)(e) propisuje da
>
> SZP može zatražiti savjet od nadzornog tijela o svim drugim pitanjima, prema potrebi.

ENZP je vrlo korisno dodatno proširio ekvivalentne obveze SZP-ova u europskim institucijama, u njihovim odnosima s ENZP-om, kako je navedeno u citatima dolje u tekstu, s tekstualnim izmjenama kako bi se koristila terminologija ENZP-a, *mutatis mutandis*, na odnos između nadzornih tijela za zaštitu podataka država članica (TZP-ova) (i ENZP-a) te SZP-ova imenovanih sukladno GDPR-u. On prije svega bilježi, općenitim terminima, da:[443]

> SZP ima zadaću odgovarati na zahtjeve [relevantnog tijela za zaštitu podataka] i, unutar sfere svoje kompetencije, surađivati s TZP-om na zahtjev potonjeg ili na vlastitu inicijativu. Ova zadaća naglašava činjenicu da SZP olakšava suradnju između [DPA] i institucije ponajprije u okviru istraga, rješavanja pritužbi ili prethodnih provjera. SZP ne samo da posjeduje unutarnje znanje (poznavanje institucije, već je vjerojatno i da zna tko je najbolja osoba za kontakt unutar institucije. SZP može također znati, i ispravno obavijestiti [DPA], o nedavnim zbivanjima koja će vjerojatno imati utjecaja na zaštitu osobnih podataka.

ENZP potom raspravlja o tome u smislu različitih pitanja spomenutih u kontekstu koji se uvelike također primjenjuje i na pitanja iz GDPR-a, kako slijedi:[444]

> **IV. Odnos SZP – [DPA]**
>
> Na postizanje sukladnosti s Uredbom će uvelike utjecati radni odnos između SZP-a i [relevantnog TZP-a]. SZP se ne smije doživljavati kao agent [TZP-a], već kao dio institucije/tijela u kojem je zaposlen/a. Kako je prethodno spomenuto, ova ideja o blizini stavlja njega/nju u idealnu situaciju za osiguravanje sukladnosti iznutra, te da pruži savjete ili intervenira u ranom stadiju time izbjegavajući moguću intervenciju nadzornog tijela. U isto vrijeme, [TZP] može ponuditi vrijednu podršku SZP-ovima u obavljanju njihove funkcije.[445]

---

442 RS29, Smjernice o SZP-ovima (bilješka 242, iznad), str. 18.

443 EDPS, Position paper on DPOs (bilješka 243, iznad), str. 6. Tekstualne izmjene u uglatim zagradama.[449] *Idem*, Dio IV (str. 10-11).

444 Idem, Dio IV (str. 10 – 11).

445 Usp. odobravanje od strane **francuskog** tijela za zaštitu podataka, CNIL, posebnog "*extraneta*" za registrirane SZP-ove, dostupna samo njima s korisničkim imenom i lozinkom, što im omogućava pravne tekstove (zakone, uredbe, itd.), kao i obuku i informacije, uključujući informacije o novim izvješćima ili smjernicama koje izda CNIL, te o drugim pravnim i praktičnim događanjima, a omogućava im da razmjenjuju mišljenja i vode diskusije. Vidi odlomak 2.3.5., pod naslovom "Formalna obuka i certificiranje" i bilješku 274, prethodno.

Od [TZP-ova se može očekivati da][446] stoga podrže[] ideju razvijanja posebnih sinergija između SZP-ova i [TZP-ova] što bi doprinijelo postizanju cjelokupnog cilja učinkovite zaštite osobnih podataka unutar institucija.…

IV. 1. Osiguravanje sukladnosti

Osiguravanje sukladnosti ponajprije započinje podizanjem svijesti. Kako se prethodno spominje, SZP-ovi igraju važnu ulogu u izgradnji znanja o pitanjima zaštite podataka unutar institucije/tijela. [Od TZP-ova se može očekivati da][447] prigrle ovo i posljedice istoga u smislu stimuliranja učinkovitog preventivnog pristupa radije negoli represivnog nadzora zaštite podatka.

SZP također pruža savjet instituciji/tijelu o praktičnim preporukama za poboljšanje zaštite podataka unutar institucije/tijela ili u pogledu tumačenja ili primjene [GDPR-a].[448] Ova savjetodavna funkcija se dijeli s [TZP-ovima] koji će savjetovati sve [svoje domaće] institucije/tijela o pitanjima koja se tiču obrade osobnih podatka ([članak 57(1)(c) GDPR-a])). Na ovom polju, [nacionalni su SZP-ovi već u prošlosti] često bili pozvani da savjetuju SZP-ove o specifičnim pitanjima vezanima za zaštitu podataka (pristup po pojedinačnom slučaju). [Od TZP-ova i ENZP-a se može očekivati] da izrade izjave o stajalištima o određenim temama kako bi pružili smjernice

institucijama/tijelima o određenim općenitijim temama.[449]

IV.2 Prethodne provjere

Mišljenja koja daje [TZP] u okviru [članka 36. GDPR-a prije konzultacija] [i gledišta TZP-ova u procesu izdavanja prethodnih odobrenja kako je predviđeno člankom 36(5)

GDPR], su također i prilika da [TZP] nadzire i osigura sukladnost s [GDPR-om]…[450]

… [P]rije konačnog usvajanja mišljenja o prethodnoj provjeri, [TZP može][451] poslati[] privremeni nacrt SZP-u s informacijama o namjeravanim preporukama time otvarajući prostor za raspravu o učinkovitosti i posljedicama namjeravanih preporuka. [Od TZP-ova se može očekivati] da brižno paze na razloge zabrinutosti institucija koje je iskazao SZP, kako bi se radilo prema praktično izvedivim preporukama.

IV. 3. Provedba

Na području provedbe pojedinih mjera zaštite podataka, javljaju se sinergijski potencijali između SZP-ova i [TZP-ova] u pogledu usvajanja sankcija i rješavanja pritužbi i upita.

Kako je prethodno spomenuto, SZP-ovi imaju ograničene ovlasti provedbe. [TZP] će doprinijeti osiguravanju sukladnosti s [GDPR-om] poduzimajući učinkovite mjere na području prethodnih [savjetovanja ili odobrenja] te pritužbi i drugih upita. Mjere su učinkovite ako su dobro usmjerene i izvedive: SZP može često biti smatran strateškim partnerom kod određivanja dobro usmjerene primjene mjere.

Rješavanje pritužbi i upita od strane SZP-a na lokalnoj razini[452] treba poticati barem u pogledu prve faze istrage i rješavanja. [Od TZP-ova se može][453] stoga [očekivati da zauzmu stav] da bi SZP-ovi

446 Izvorna rečenica kaže da ENZP "podržava" ideju. Može se očekivati da će TZP-ovi (i EOZP) zauzeti isti stav.
447 Izvorna rečenica kaže da ENZP "pozdravlja" ovaj pristup, ali (također u svjetlu najbolje prakse), opet se može očekivati da će TZP-ovi (i EOZP) zauzeti isti stav.
448 Referenca u ENZP-ovom radu je na regulativu koja postavlja pravila zaštite podataka za same EU institucije (Uredba (EC) 45/2001) (bilješka 148, iznad), ali isto naravno vrijedi i u odnosu na GDPR, što se tiče SZP-ova imenovanih po toj naknadnoj regulativi. Mi smo napravili slične zamjene drugdje u citatu.
449 Izvorna rečenica kaže da ENZP "namjerava izraditi" rad o stavu i smjernice. Ponovo, može se očekivati da će nacionalni TZP-ovi i EOZP učiniti istu u odnosu na GDPR.
Ispuštena rečenica glasi: "U pogledu SZP-ova imenovanih na osnovi GDPR-a, nacionalni TZP-ovi, ali posebno novi EOZP, će nesumnjivo izdati slične smjernice."
450 Ostatak ovog stavka, i ispuštena rečenica na početku sljedećeg stavka, bave se činjenicom da je vremenski jaz između stupanja na snagu Uredbe i imenovanja ENZP-a stvorio veliki zaostatak predmeta koji se "prethodno pregledavaju" po "ex post" osnovi. Još nije jasno javljaju li se isti problemi prema GDPR-u. Ako da, ENZP-ovi pozivi SZP-ima i regulatoru da budu "strateški partneri" u rješavanju ovoga treba također biti sagledana u tom kontekstu.
451 Praksa slanja "privremenih nacrta preporuka" voditelju obrade u kontekstu procesa "prethodnog savjetovanja"/ "prethodnog odobrenja" nije navedena u GDPR-u (ni Uredbi 45/2001). Međutim, sama činjenica da se GDPR referira na "prethodno *savjetovanje*" snažno ukazuje na do da će TZP-ovi, prema tom instrumentu, zauzeti sličan pristup; a to se odražava u terminima unutar uglatih zagrada dva puta dodanih u ovom stavku.
452 Primijetite da rješavanje zahtjeva i pritužbi ispitanika je dalje raspravljeno u 11. zadaći, dalje u tekstu.
453 Prve dvije rečenice u ovom stavku opet se odnose na praksu koju promovira ENZP – ali opet je (također u skladu s prošlom praksom) u cijelosti za očekivati da će nacionalni TZP-ovi zauzeti isti pristup (kako je navedeno u tekstu unutar uglate zagrade).

trebali pokušati istražiti i riješiti pritužbe na lokalnoj razini prije slanja [TZP-u]. SZP bi također trebao … konzultirati [TZP] kad god on/a ima sumnje oko procedure ili sadržaja pritužbi. To, međutim, ne sprječava ispitanika da se izravno obrati [TZP-u] sukladno [članku 77(1) GDPR-a]. Ograničene ovlasti provedbe SZP-a također imaju implikaciju da u nekim slučajevima, pritužba ili upit moraju biti poslani na višu instancu [TZP-u]. [TZP] stoga osigurava vrijednu podršku na području provedbe. Zauzvrat, može se osloniti da će SZP pružiti informacije [TZP-u] i dostaviti naknadno stanje usvojenih mjera.

IV.4. Mjerenje učinkovitosti[454]

Što se tiče mjerenja učinkovitosti primjene zahtjeva zaštite podataka, SZP se mora smatrati korisnim partnerom za procjenu napretka na ovom području. Primjerice, kad dođe do mjerenja izvedbe internog nadzora zaštite podataka, [od TZP-ova se može očekivati da će] poticati[] SZP-ove da razviju svoje vlastite kriterije dobrog nadzora

(profesionalni standardi, specifični planovi za instituciju, godišnji plan rada …). Ovi će

kriteriji zauzvrat omogućiti [TZP-u], kada je tijelo pozvano to učiniti, da procijeni rad SZP-a, ali će također služiti kako bi mu omogućila da mjeri stanje primjene [GDPR-a] unutar institucije/tijela.

Također je vjerojatno da će SZP-ovi u javnom sektoru biti pozvani od strane njihovih TZP-ova da daju svoj doprinos savjetovanjima koja provode TZP-ovi te da doprinesu pripremi formalnih mišljenja ili nacrtu zakona u području zaštite podataka koji se tiču okolnosti u kojima SZP-i djeluju.

Na kraju, treba primijetiti da SZP igra važnu ulogu u pomaganju TZP-u u provođenju nadzora na licu mjesta, uz savjetovanje SZP-a s voditeljima obrade u specifičnim sektorima, itd. Primjerice, rijetko je da TZP-ovi provode inspekcije bez najave – to se doista radi samo u odnosu na sumnju na zločince koji mogu sakriti podatke ili druge dokaze ako bi unaprijed dobili upozorenje o inspekciji. U praksi, TZP-ovi uobičajeno prethodno dogovore inspekcije uz pomoć voditelja obrade, a posebice voditeljevog SZP-a, koji će biti u mogućnosti osigurati da su prave osobe dostupne i da se mogu pregledati pravi sustavi. Ovo je često od ključne važnosti, posebno u odnosu na složene sustave obrade, gdje je dubinsko poznavanje ICT arhitekture i internih procesa potrebno za pravilno preispitivanje. A kada TZP želi detaljno pregledati obradu osobnih podataka u posebnom kontekstu ili sektoru – što mnogi i čine prema godišnje određenom planu i odabiru prioriteta – oni će se obratiti SZP-ovima voditelja obrade aktivnih u kontekstu ili sektoru radi stvarnog uvida, održavajući sastanke s njima i pitajući ih za odgovore na savjetovanje. I ovo je dio onoga što ENZP naziva "strateško partnerstvo" između SZP-ova i TZP-ova.

454 Ne postoje posebni zahtjevi, ni u Uredbi 45/2001 (u pogledu EU institucija), ni u GDPR-u (u pogledu pravnih osoba obuhvaćenih tim instrumentom), za relevantnog regulatora (odnosno, ENZP i nacionalni TZP-ovi) da "mjere učinkovitost" mjera koje je usvojio voditelj obrade s ciljem osiguravanja sukladnosti s važećim instrumentom. Unutar EU institucionalnog okvira, ENZP ipak (s pravom) vidi ovo kao prirodan dio svojeg posla. Za očekivati je da će TZP-ovi država članica (i ENZP) također "poticati" SZP-ove da doprinesu visokim stupnjem sukladnosti kroz usvajanje ili priključivanje "profesionalnim standardima, posebnim planovima za instituciju, godišnjim programom rada" itd.; kao što se opet ogleda u terminologiji unutar uglatih zagrada.

RJEŠAVANJE ZAHTJEVA ISPITANIKA

13. ZADAĆA: Rješavanje zahtjeva i pritužbi ispitanika

GDPR propisuje da:

> Ispitanici mogu kontaktirati službenika za zaštitu podataka u pogledu svih pitanja povezanih s obradom svojih osobnih podataka i ostvarivanja svojih prava iz ove Uredbe (čl. 38(4)).

Ispitanici koji žele ostvariti bilo koje od svojih **prava ispitanika** – prava na pristup, ispravak i brisanje ("pravo na zaborav"), ograničenje obrade, prenosivost podataka, pravo prigovora općenito i u odnosu na automatizirano donošenje odluka, uključujući izradu profila – u pogledu organizacije, ili oni koji imaju **opća pitanja** ili **pritužbe** vezane za zaštitu podataka o organizaciji, trebali bi se uobičajeno prvo obratiti SZP-u te organizacije (kada isti/a postoji).

Ovo je olakšano zahtjevom iz GDPR-a da je organizacija dužna objaviti kontaktne podatke SZP-a (čl. 37(7)) i da voditelj obrade mora osigurati "*da je službenik za zaštitu podataka na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka [koji se odnose na organizaciju]*" (čl. 38(1)). (Stoga, ako se ispitanik želi obratiti nekome u organizaciji, kao što je glavni pravni savjetnik ili glavni direktor, oni bi trebali proslijediti zahtjev SZP-u.)

Štoviše, neovisan status SZP-a (čl. 38(3)) bi trebao osigurati da zahtjev, upit ili pritužbu rješava SZP – ili odgovoran zaposlenik pod nadzorom SZP-a – **na primjeren način, bez predrasuda u korist organizacije ili protiv ispitanika**. U svakom slučaju, SZP bi trebao/la ili sam/a napisati ili pregledati odgovor ispitaniku. Ovo bi trebalo uključivati savjet da, ako ispitanik nije zadovoljan odgovorom, onda se može obratiti s tim pitanjem TZP-u.

Razlog ovome je, u svakom slučaju, pravo ispitanika da podnesu zahtjeve, upite i pritužbe organizaciji (tj. SZP-u organizacije) **bez štete za njihovo pravo na pritužbu nadzornom tijelu**. Posebno, od svakog TZP-a se traži i ovlašteno je, na svom području, činiti sljedeće:

> rješava pritužbe koje podnos[i] ispitanik … i istražuje u odgovarajućoj mjeri predmet pritužbe te podnositelja pritužbe u razumnom roku izvješćuje o napretku i ishodu istrage … (čl. 57(1)(f))

U takvim pritužbama TZP-u, ispitanike mogu zastupati neprofitno tijelo (čl. 80), a gornja obveza i ovlast TZP-a za rješavanje takvih pritužbi proširuje se na slučajeve pokrenute na taj način (vidi terminologiju u članku 57(1)(f), ispušteno iz gornjeg citata).

U tom svjetlu, imalo bi smisla da SZP-ovi budu voljni riješiti zahtjeve i **pritužbe takvih zastupničkih organizacije**, a ne samo od ispitanika.

Kako je već navedeno u odnosu na 10. zadaću (*Suradnja s TZP-om*), za očekivati je (također u svjetlu prošlog iskustva) da će nacionalni TZP-ovi (kao i ENZP u odnosu na SZP-ove EU institucija) poticati ispitanike (i takve organizacije) da se uvijek prvo s predmetom obrate voditelju obrade, točnije njegovom SZP-u, kako bi provjerili može li se predmet već zadovoljavajuće istražiti i riješiti bez takvih interakcija, bez uključivanja TZP-a, pod uvjetom da bi SZP trebao pitati za savjet TZP ako se jave bilo koja pitanja o općem tumačenju i primjeni GDPR-a. Ali ovo nikada ne bi trebalo ići tako daleko da se na kraju obeshrabri ispitanike (ili zastupničke organizacije) od postavljanja pitanja – i naravno posebno načelnih pitanja – kod TZP-a.

Kako je ENZP rekao, regulator i SZP-ovi su u "strateškom partnerstvu": TZP-ovi mogu potaknuti ispitanike da se prvo i ponajprije srede bilo koja pitanja izravno sa SZP-om; a SZP-ovi moraju biti u mogućnosti – i to se od njih traži – raditi s regulatorom kako bi se osiguralo da odgovori na pitanja i pritužbe budu pravilno riješeni, a po potrebi i dovesti do promjena u relevantnoj praksi voditelja obrade. TZP-ovi moraju biti u mogućnosti osloniti se na SZP-ove kako bi doista podržali ispitanike s bilo kojom pritužbom; a SZP-ovi se moraju moći osloniti na TZP-ove kako bi osigurali da se preporuke za promjenu doista i provedu.

Ovo sve povećava delikatnost pozicije SZP-a, raspravljenu u Drugom dijelu, pod točkom 2.5: SZP-ovi su most između voditelja obrade i regulatora – i (iako je to donekle pomiješana metafora, osim ako netko riječ "most" pročita kao "uska pasarela za ulazak na jedrilicu") ne bi se trebao dopustiti pad između jedrilice i mola.

INFORMIRANJE I PODIZANJE SVIJESTI

14. ZADAĆA: Zadaće internog i vanjskog informiranja, te zadaća podizanja svijesti

GDPR navodi da će zadaće SZP-a uključivati "barem"

> Informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka (čl. 39(1)(a))

Interno (unutar organizacije gdje je SZP zaposlen), ovo implicira, s jedne strane, da SZP **informira** zaposlenike o njihovim pravima i, s druge strane, SZP **daje upute** voditeljima obrade i organizaciji i zaposlenicima – uključujući posebice "vlasnike posla"/osobe odgovorne za pojedine postupke obrade – o njihovim obvezama i odgovornostima te **osposobljavanje** tih osoba oko udovoljavanja tim zahtjevima.

Kako ENZP kaže u odlomku koji je citiran već prethodno:[455]

> Osiguravanje sukladnosti započinje podizanjem svijesti. … SZP-ovi igraju važnu ulogu u razvoju znanja pitanjima zaštite podatka unutar institucije/tijela.

Podizanje svijesti "stimulira učinkovit preventivni pristup, a ne represivni nadzor zaštite podataka".[456]

Mjere koje usvoji SZP prema tim ciljevima mogu uključivati izdavanje **informativnih bilješki za zaposlenike**, organiziranje internih **satova osposobljavanja** za zaštitu podataka – koji bi trebali imati za cilj ugraditi u zaposlenike svijest i senzibilitet prema zaštiti podataka i pravima ispitanika – "refleks zaštite podataka" – u svim njihovim različitim ulogama u društvu, bilo kao običan građanin, radnik, vođa tima ili direktor.

Također, postavljanje internih **mrežnih stranica** s internim informacijama o zaštiti podataka i podukom o tim pitanjima, te sastavljanje i objava **izjava o privatnosti** na mrežnim stranicama osoblja.[457]

Vanjski, izuzev osiguravanja da su ispitanici dobili relevantne informacije kada su se podaci o njima prvi puta prikupljali (kako je navedeno u člancima 12 – 14 GDPR-a), npr. na jasnim mrežnim obavijestima, SZP bi uvijek trebao raditi sa svim osobljem za odnose s javnošću kako bi se osigurala **potpuna transparentnost o postupcima obrade osobnih podataka unutar organizacije**: o svrhama za koje prikuplja i obrađuje osobne podatke; kategorijama ispitanika i uključenih podataka; primateljima podataka; prenose li se podaci u treće (izvan EU/EGP) zemlje itd.

GDPR ne traži od voditelja obrade koji vode evidenciju aktivnosti obrade osobnih podataka da to bude u cijelosti dostupno javnosti.[458] Međutim, GDPR to svakako ne zabranjuje.

ENZP snažno zagovara u korist objave u odnosu na EU institucije, posebice u svjetlu činjenice da (kao Direktiva o zaštiti podataka iz 1995. g.) je raniji propis zahtijevao od njih da objave svoje "funkcionalno ekvivalentne" pojedinosti o obavijesti:[459]

---

455 ENZP, Position paper on DPOs (bilješka 243, iznad), str. 10.
456 *Idem*.
457 *Idem*, str. 5.
458 Nasuprot tome, Direktiva o zaštiti podataka iz 1995. nije zahtijevala od TZP-ova da bilježe detalje postupaka obrade o kojima su obaviješteni javnim putem (čl. 21).
459 EDPS, Accountability on the ground (bilješka 353, iznad), str. 8, izvorni naglasak.

Evidencije su važan alat za provjeru i dokumentiranje da Vaša organizacija kontrolira svoje aktivnosti obrade podataka…

ENZP snažno preporučuje da [EU institucije] učine evidencije javno dostupnima, po mogućnosti objavom na mrežnim stranicama …

Postoji mnogo razloga zašto bi registar evidencija trebao biti javan:

- doprinosi transparentnosti EUI-a12;
- pomaže ojačati javno povjerenje;
- olakšava dijeljenje znanja između EUI-a;
- neobjavljivanje toga bilo bi korak unatrag iza starih [pravila].

Prilično se isto može reći u odnosu na registar postupaka obrade kojeg trebaju voditi voditelji obrade prema GDPR-u – u najmanju ruku, barem što se tiče javnih tijela. Neke države članice mogu u svojem nacionalnom zakonu nametnuti takvu obvezu objave pojedinosti iz evidencije; ali javne vlasti u državama gdje to nije obvezno bi i dalje uvijek trebale razmatrati učiniti isto u svjetlu opažanja ENZP-a.

Naravno, voditelji obrade i izvršitelji obrade se ne bi trebali osjećati obvezni objaviti informacije o svojim sigurnosnim aranžmanima koji bi se mogli koristiti za povredu upravo te sigurnosti (ovo je već priznato u odredbi Direktive o zaštiti podataka iz 1995. g., vezano za objavu pojedinosti o postupcima obrade koji su prijavljeni TZP-ima).[460]

Osnovne informacije o postupcima obrade osobnih podataka organizacije trebaju u svakom slučaju biti dostupne na **mrežnim stranicama** organizacije te također pružene u **biltenima** i **formularima** (uključujući verzije dostupne i osobama s invaliditetom).

Mrežne stranice i takve forme bi također trebale jasno pružati informacije o tome **kako ispitanici mogu ostvariti svoja prava** (uključujući jasnu javnu obavijest s **kontaktnim podacima SZP-a** – premda to ne treba uključivati ime); kojih **kodeksa ponašanja** se pridržava organizacija i koji su mehanizmi certificiranja odobreni (ova pitanja se mogu prikazati putem priznatih **oznaka** ili **pečata**) itd.

Bilo koje mrežne stranice bi, naravno, također trebale u cijelosti zadovoljavati zahtjeve EU prava zaštite podataka, kao i bilo kojih relevantnih daljnjih nacionalnih zakona, po pitanju recimo **kolačića** (*cookies*) i drugog ***tracker*** softvera itd.

460 Vidi ponovo članak 21 iz Direktive o zaštiti podataka iz 1995., koja isključuje informacije navedene u članku 19(1)(f) – tj. opći opis sigurnosnih mjera voditelja obrade – od informacija koje treba javno objaviti.
Međutim, primijetite da je uvjerenje da stoji "sigurnost kroz neprozirnost", vidi: https://en.wikipedia.org/wiki/Security_through_obscurity

ZADAĆA 15. *Planiranje i pregled aktivnosti SZP-a*

Konačno, s obzirom na veliki broj i opseg zadaća SZP-a, isti bi trebali pripremiti godišnje izvješće svojih aktivnosti, uzimajući u obzir vrijeme potrebno za obavljanje svake od njih i posvetiti se predvidivim novim unapređenjima te istovremeno odvojiti vrijeme za nepredviđene događaje; kao i redovito revidirati i ažurirati ovaj plan.

Douwe Korff & Marie Georges

Cambridge/Paris, lipanj 2019.