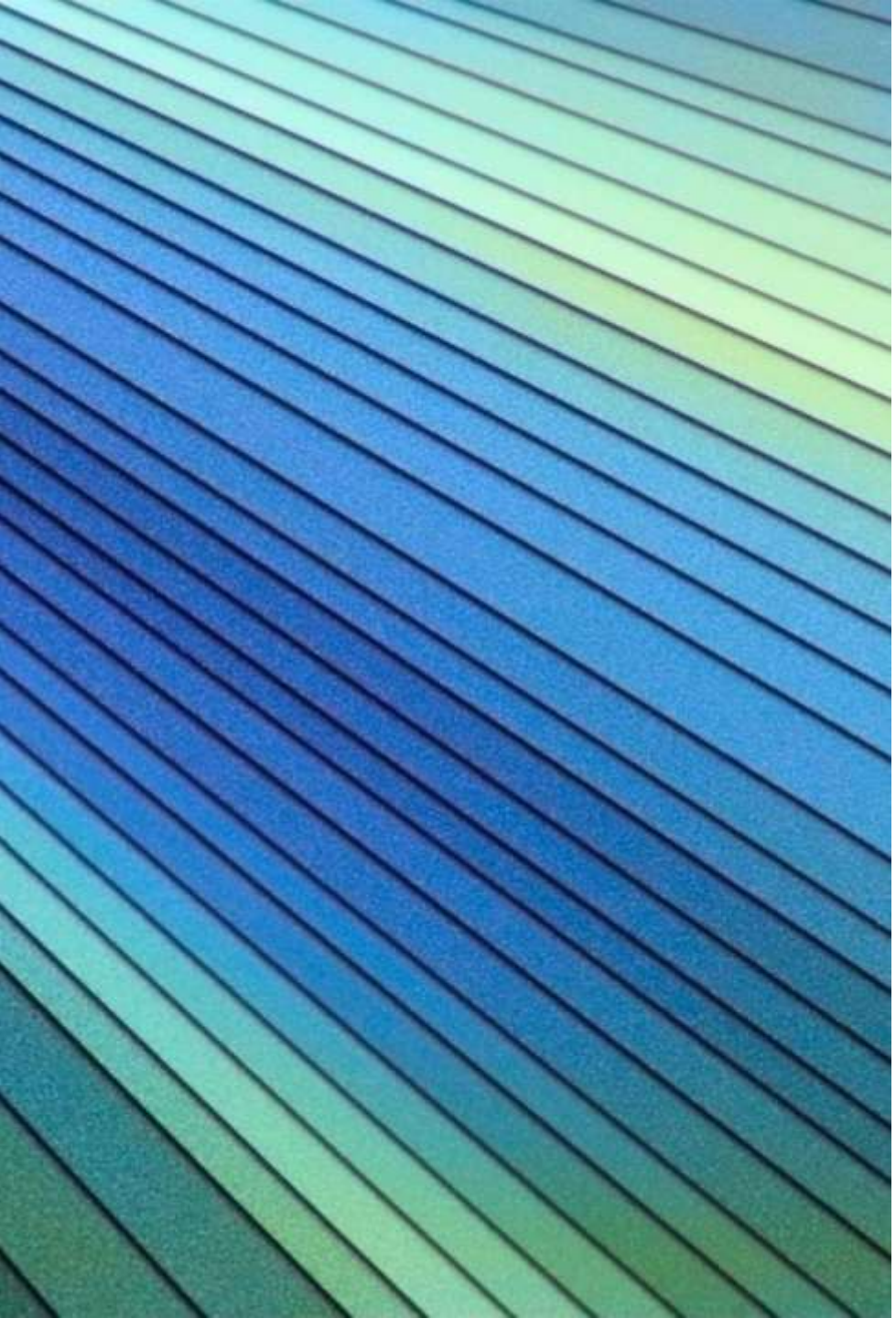
# SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA- OSNOVNI MODUL



# Imenovanje službenika- ZZOP

01

**od 2012.** godine definiran Zakonom o zaštiti osobnih podataka

02

**čl. 18.a ZZOP-a** službenik za zaštitu osobnih podataka

03

**od 25. svibnja 2018.** ODREDBA PRESTAJE VAŽITI

# Imenovanje službenika – OPĆA UREDBA

- Voditelj/izvršitelj obrade **imenuju** službenika **u 3 slučaja:**

1. **Ako obradu provodi tijelo javne vlasti ili javno tijelo** (bez obzira na to koji se podaci obrađuju), osim za sudove

   → Tijelo javne vlasti definirano Zakonu o provedbi Opće uredbe
2. Ako se osnovne djelatnosti obrade sastoje od postupaka obrade koji iziskuju **redovito i sustavno praćenje ispitanika u velikoj mjeri**
3. Ako se osnovne djelatnosti obrade sastoje od opsežne obrade **posebnih kategorija podataka** ili osobnih podataka koji se odnose na **kaznene osude i kažnjiva djela**

# PREPORUKA

- ako Općom uredbom nije izričito propisano imenovanje službenika, za poslovne subjekte može biti korisno **dobrovoljno imenovanje**

# SMJERNICE Radne skupine iz čl.29

- Smjernice o Službeniku za zaštitu osobnih podataka objavljene na službenoj web stranici Agencije
- https://azop.hr/images/dokumenti/217/wp243rev01_hr.pdf

- Sve odluke o imenovanju službenika donesene na temelju starog Zakona o zaštiti osobnih podataka **trebaju se uskladiti s Uredbom**

- Imenovanje službenika za zaštitu podataka mora biti u pisanom obliku i dostavljeno u izvorniku s potpisom i pečatom odgovorne osobe na sjedište Agencije: Selska cesta 136, 10000 Zagreb

OBRAZAC: https://azop.hr/zbirke-osobnih-podataka/detaljnije/registar-sluzbenika-za-zastitu-osobnih-podataka

***IZVJEŠĆE***

***o imenovanju službenika za zaštitu podataka***

*temeljem članka 37. UREDBE (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)*

* Voditelj/Izvršitelj obrade:

(navesti registrirani službeni naziv Voditelja/Izvršitelja obrade i naznaku radi li se o Voditelju ili Izvršitelju obrade)

* Sjedište Voditelja/Izvršitelja obrade:

(navesti adresu, poštanski broj i mjesto sjedišta Voditelja/Izvršitelja obrade)

* OIB Voditelja/Izvršitelja obrade: *Dana:

(navesti OIB Voditelja/Izvršitelja obrade) (navesti nadnevak donošenja odluke o imenovanju)

**donio je Odluku o imenovanju službenika za zaštitu podataka:**

* Ime i prezime:

(navesti puno ime i prezime službenika za zaštitu podataka)

* Adresa i mjesto rada:

(navesti adresu, poštanski broj i mjesto rada službenika za zaštitu podataka, te navesti svojstvo - ukoliko se funkcija obavlja temeljem Ugovora o djelu)

*Telefon: *e-mail:

(navesti broj telefona za kontakt službenika za zaštitu podataka) (navesti e-mail adresu za kontakt službenika za zaštitu podataka)

Mjesto: Dana:

* M.P. *

(Klasa, Urbroj i ostali neobvezni podaci) (pečat Voditelja/Izvršitelja obrade – ako je primjenjivo) (potpis odgovorne osobe kod Voditelja/Izvršitelja obrade)

https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/

# Mogu li organizacije zajednički imenovati službenika?

Skupina poduzetnika **može imenovati jednog službenika** pod uvjetom da je isti **"lako dostupan iz svakog poslovnog nastana"**

## UVJETI:

Važno osigurati da su njegovi **podaci za kontakt lako dostupni**

Mora moći **učinkovito komunicirati** s ispitanicima i surađivati s predmetnim nadzornim tijelima → komunikacija se mora odvijati na jeziku koji upotrebljava predmetno nadzorno tijelo i ispitanici

**Osobna dostupnost** (fizička, telefonskim putem ili drugim sredstvima komunikacija)

# Vanjski službenik za zaštitu osobnih podataka

- Službenik može biti član osoblja voditelja ili izvršitelja obrade (unutarnji službenik) ili “**obavljati zadaće na temelju ugovora o djelu**” tj. može biti vanjski službenik

# Stručne kvalifikacije službenika

- Općom uredbom propisano je da se službenik imenuje **na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka** te **sposobnosti izvršavanja zadaća** iz članka 39. Opće Uredbe

# POTREBNE VJEŠTINE I STRUČNOST

- Stručnost u pogledu **nacionalnih i europskih zakona i praksi u području zaštite podataka** (uključujući dubinsko razumijevanje GDPR-a)
- Razumijevanje **provedenih postupaka obrade**
- Razumijevanje **informacijskih tehnologija i sigurnosti podataka**
- **Poznavanje poslovnog sektora i organizacije**
- **Sposobnost promicanja kulture zaštite podataka** unutar organizacije

# RADNO MJESTO SLUŽBENIKA

SUDJELOVANJE SLUŽBENIKA U SVIM PITANJIMA KOJA SE ODNOSE NA ZAŠTITU OSOBNIH PODATAKA

Čl. 38. st.1 Opće uredbe - voditelj/izvršitelj obrade osiguravaju da službenik **„na primjeren način i pravodobno bude uključen u sva pitanja u pogledu zaštite osobnih podataka"**

**Važno –** što ranije biti uključen u sva pitanja koja se odnose na zaštitu osobnih podataka

**Prijedlog –** da službenik bude dio relevantnih radnih skupina koje se unutar organizacije bave poslovima obrade osobnih podataka

PREPORUKE:

- **Sudjelovanje na redovitim sastancima visokog i srednjeg rukovodstva**
- **Nazočnost kada se donose odluke koje se mogu odraziti na zaštitu osobnih podataka**
- **Uvažiti mišljenje službenika**
- **Savjetovanje sa Službenikom nakon što dođe do povrede osobnih podataka**

# RADNO MJESTO SLUŽBENIKA

## POTREBNA SREDSTVA ZA RAD

Čl. 38. st. 2 Opće uredbe – podupiranje službenika **„pružajući mu potrebna sredstva za izvršavanje njegovih zadaća i ostvarivanje pristupa osobnim podacima i postupcima obrade te za održavanje njegovog stručnog znanja”**

- **Aktivna potpora visokog rukovodstva (na razini upravnog odbora)**
- potrebno osigurati **dovoljno vremena** za ispunjavanje njihovih zadaća
- Osigurati odgovarajuću potporu u smislu financijskih sredstava, infrastrukture (poslovni prostori, objekti, oprema) i, prema potrebi, osoblja
- Osigurati da se svom osoblju dostavi službena obavijest o imenovanju službenika za zaštitu podataka
- Omogućiti nužan pristup ostalim službama ( ljudski resursi, pravna služba, informacijske tehnologije, sigurnost itd)
- **Omogućiti kontinuirano osposobljavanje – unaprjeđivanje razine stručnosti**
- s obzirom na veličinu i ustroj organizacije, moglo bi biti potrebno uspostaviti jedinicu službenika za zaštitu podataka (službenik za zaštitu podataka i njegova jedinica)

# RADNO MJESTO SLUŽBENIKA

DAVANJE UPUTA I „OBAVLJANJE SVOJE DUŽNOSTI I ZADAĆA NA NEOVISAN NAČIN”

Čl 38. st 3. od voditelja obrade/izvršitelja obrade zahtijeva se da osiguraju da službenik za zaštitu podataka **„ne prima nikakve upute u pogledu izvršenja [svojih] zadaća”**

U uvodnoj izjavi 97. - službenici za zaštitu podataka, **„bez obzira jesu li zaposlenici voditelja obrade, trebali [...] moći obavljati svoje dužnosti i zadaće na neovisan način”**

To znači da se službenicima **ne smiju davati upute** o načinu rješavanja predmeta (npr. o ishodu koji bi trebalo ostvariti, načinu vođenja istrage o pritužbi ili o tomu treba li tražiti savjet nadzornog tijela.)

Ako voditelj/izvršitelj obrade donese odluke nespojive s Općom uredbom i savjetom službenika, trebalo bi omogućiti službeniku da svoje suprotno mišljenje jasno da do znanja najvišoj rukovodećoj razini te onima koji donose odluke

# RADNO MJESTO SLUŽBENIKA

RAZRJEŠENJE DUŽNOSTI ILI KAZNA ZBOG IZVRŠAVANJA ZADAĆA SLUŽBENIKA ZA ZAŠTITU PODATAKA

U skladu s čl. 38. st. 3. voditelj ili izvršitelj obrade „ne smiju [službenika za zaštitu podataka] razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća”

Pojačava se autonomija službenika te se pomaže osigurati neovisnost njihova djelovanja

Kazne mogu biti izravne i neizravne

Preporuka – što bolje definiranje zadaća i ovlasti službenika ugovorom o radu

# MOGUĆI SUKOB INTERESA

Opća uredba propisuje da službenik **„može ispunjavati i druge zadaće i dužnosti”** međutim, zahtijeva da organizacija osigura da **„takve zadaće i dužnosti ne dovedu do sukoba interesa”**

**→ USKO POVEZANO SA OBVEZOM DJELOVANJA NA NEOVISAN NAČIN**

**RADNA MJESTA KOJA MOGU BITI U SUKOBU INTERESA U OKVIRU POSLOVNOG NASTANA:**

**Položaji u višem rukovodstvu** (predsjednik uprave, direktor poslovanja, direktor financija, glavni medicinski službenik, voditelj odjela za marketing, voditelj ljudskih resursa ili voditelj odjela za infomacijsku tehnologiju)

**Niže uloge u hijerarhijskoj strukturi poslovnog nastana** ako takvi položaji ili uloge podrazumijevaju utvrđivanje svrhe i načina obrade osobnih podataka

# PRAĆENJE USKLAĐENOSTI SA OPĆOM UREDBOM

- Konkretno, u okviru dužnosti praćenja poštovanja Opće uredbe službenik za zaštitu podataka može:

  - ✓ **Prikupljati informacije radi utvrđivanja aktivnosti obrade**
  - ✓ **Analizirati i provjeravati usklađenost aktivnosti obrade**
  - ✓ **Obavješćivati voditelja/izvršitelja obrade te mu pružati savjete i izdavati preporuke**

# ZADAĆE

**informiranje i savjetovanje** voditelja ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe

**praćenje poštovanja ove Uredbe** te drugih odredaba Unije ili DČ o zaštiti podataka i politika voditelja ili izvršitelja obrade u odnosu na zaštitu osobnih podataka

**pružanje savjeta u pogledu procjene učinka** na zaštitu podataka i praćenje njezina izvršavanja

**suradnja s nadzornim tijelom**

**djelovanje kao kontaktna točka** za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje

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

# ODGOVORNOST?!

- **<u>Službenici nisu osobno odgovorni za nepoštovanje Opće uredbe</u>**

→ Osiguravanje usklađenosti zaštite podataka s njezinim odredbama dužnost je voditelja ili izvršitelja obrade

# ULOGA I ZADAĆE SLUŽBENIKA U POSTUPKU IMPLEMENTACIJE OPĆE UREDBE

# Neke od zadaća

1. **Prava ispitanika i rješavanje povreda**
2. **Interni akti**
3. **Procjena rizika i provođenje procjene učinka na zaštitu podataka**
4. **Suradnja s nadzornim tijelom**

# PRAVA ISPITANIKA – GDPR

- **KOJA PRAVA POSTOJE?**
- **PRAVO NA PRISTUP OSOBNIM PODACIMA (KOJI SE ODNOSE NA IPITANIKA)**
- **PRAVO NA ISPRAVAK**
- **PRAVO NA BRISANJE** („pravo na zaborav”)
- **PRAVO NA OGRANIČENJE OBRADE**
- **PRAVO NA PRENOSIVOST PODATAKA** („data portability”)
- **PRAVO NA PRIGOVOR**
- **PRAVO USPROTIVITI SE DONOŠENJU AUTOMATIZIRANIH POJEDINAČNIH ODLUKA, UKLJUČUJUĆI IZRADU PROFILA**

- **→ pravo na zaštitu osobnih podataka NIJE APSOLUTNA**
- **→ test ravnoteže sa ostalim pravima**

- **PRAVO NA PRISTUP**

  - članci 12., 13. i 14. GDPR-a sadrže popis informacija koje se trebaju pružiti ispitanicima

  - kad je obavijest o privatnosti  jasna i transparentna, to povećava povjerenje ispitanika te smanjuje upite ispitanika

- **PRAVO NA PRISTUP**

- pravo na pristup (članak 15. GDPR-a)  obuhvaća ispitanika pravo dobiti od voditelja obrade potvrdu: jesu li osobni podaci obrađeni i ako je tako, dobiti pristup i/ili kopiju obrađenih osobnih podataka
- Ispitanik ima pravo dobiti informacije iz čl. 15.
  - → SVRHA OBRADE
  - → KATEGORIJE OSOBNIH PODATAKA
  - → PRIMATELJI ILI KATEGPRIJE PRIMATELJA
  - → ROKOVI ČUVANJA
  - → PRAVO NA ISPRAVAK/BRISANJE ILI OGRANIČAVANJE OBRADE
  - → PODNOŠENJE PRITUŽBE NADZORNOM TIJELU
  - → O IZVORU PRIKUPLJANJA OSOBNIH PODATAKA
  - → POSTOJANJE AUTOMATIZIRANOG DONOŠENJA ODLUKA, UKLJUČUJUĆI IZRADU PROFILA

# PRAVO NA ISPRAVAK

- ispitanik ima pravo bez odgađanja ostvariti kod voditelja obrade ispravak netočnih podataka

→ **Ažurni  i točni podaci = uvjet za zakonitu i valjanu obradu**

## PRAVO NA BRISANJE/“PRAVO NA ZABORAV“

***Presuda Suda Europske unije u slučaju Google vc Costeja C-131/12***

- omogućeno da se od Internet tražilica ishodi trajno uklanjanje određenih rezultata pretrage (osobnih podataka)

**ISPITANIK IMA PRAVO ISHODITI BRISANJE AKO:**


✓ osobni podaci više nisu nužni u odnosu na svrhu za koju su prikupljeni
✓ je privola povučena
✓ uložen je prigovor na obradu
✓ su osobni podaci nezakonito obrađeni
✓ osobni podaci moraju se brisati radi poštovanja pravne obveze (pravo EU ili države članice)
✓ osobni podaci su prikupljeni u vezi s ponudom usluga informacijskog društva iz članka 8. (1)

✓ **IZNIMKE**
→ kada OP nisu nužni za ostavarivanje na slobodu izražavanja i na slobodu informiranja;
→ radi poštovanja pravnih obveza;
→ radi izvršavanja zadaća od javnog interesa u području javnog zdravlja,
→ u svrhe arhiviranja od javnog značaja itd.

- **PRAVO NA OGRANIČENJE OBRADE**

- članak 18. GDPR-a
- Ispitanik može tražiti od voditelja obrade da privremeno ograniči obradu osobnih podataka ako:
- se osporava točnost osobnih podataka;
- obrada je nezakonita i ispitanik zahtijeva ograničenje umjesto brisanja;
- podaci se moraju čuvati za ostvarivanje ili obranu pravnih zahtjeva;
- čeka se potvrda o legitimnim interesima voditelja obrade podataka koji prevladavaju nad interesima ispitanika

# PRAVO NA PRENOSIVOST PODATAKA

- **svaki građanin ima pravo samostalno izabrati pružatelja usluge a uvođenjem novog prava ispitanicima se omogućuje da zaprime osobne podatke koje su pružili jednom voditelju obrade te ih ustupe drugom voditelju**

- **Npr. – teleoperateri**

## PRAVO NA PRENOSIVOST PODATAKA

- članak 20. GDPR-a

→ ispitanici uživaju pravo na prijenos podataka u situacijama kada se osobni podaci obrađuju:

- automatiziranim sredstvima na temelju privole
- ili kada je obrada neophodna za izvršenje ugovora i provodi se automatiziranim sredstvima
- ako je tehnički izvedivo

# PRAVO NA PRIGOVOR

-ispitanik ima pravo na temelju  svoje posebne situacije na prigovor u svakom trenutku obrade podataka koji se na njega odnose uključujući i izradu profila

- kada se osobni podaci obrađuju za potrebe direktnog marketinga ispitanik ima pravo u svakom trenutku uložiti prigovor na obradu osobnih podataka za svrhe konkretnog marketinga uključujući i izradu profila povezanu s konkretnim marketingom

# AUTOMATIZIRANE POJEDINAČNE ODLUKE I PROFILA

-ispitanik ima pravo da se na njega **ne odnose odluke koje se temelje isključivo na automatiziranoj obradi uključujući i profiling**

- ispitanik **<u>može biti subjekt</u>** takvih odluka u slučaju :
1) potrebe za sklapanjem ili izvršenjem ugovora između ispitanika i voditelja obrade
2) ako je isto dopušteno pravom Unije ili DČ
3) ako je obrada utemeljena na izričitoj privoli

AUTOMATIZIRANO DONOŠENJE ODLUKA događa se kad se odluke o vama donose tehnološkim sredstvom i bez bilo kakve uključenosti čovjeka.

PRIMJER: izračunavanje kreditnog rejtinga putem bankovne aplikacije

PROFIL se izrađuje kad se vaši osobni aspekti procjenjuju kako bi se sastavila predviđanja o vama, čak i ako se ne donosi nikakva odluka.

PRIMJER: ako društvo ili organizacija procjenjuje vaše karakteristike (poput vaše dobi, spola, visine) ili ako vas razvrsta u kategoriju, to znači da vam se izrađuje profil.

# OBVEZE VODITELJA OBRADE

-poduzeti odgovarajuće mjere kako bi se ispitaniku:

- ✓ **pružile sve informacije iz čl. 13. i 14.**
- ✓ **sva komunikacija iz čl. 15-22. i čl. 34 u vezi s obradom**

# DAVANJE INFORMACIJA ISPITANIKU

- **voditelj obrade pruža informacije bez odgode o poduzetim radnjama iz čl. 15- 22. Opće uredbe**

- **rok: 30 dana od dana zaprimanja zahtjeva**

- **po potrebi rok se može produljiti za još 2 mjeseca**

- **voditelj obrade je obvezan o svakom takvom produljenju izvijestiti ispitanika**

**(rok mjesec dana od zaprimanja zahtjeva + razloge odgađanja)**

# NEPOSTUPANJE PO ZAHTJEVU ZA OSTVARIVANJE PRAVA

**Ako voditelj obrade ne postupi po zahtjevu on bez odgađanja (najkasnije 1 mj od zaprimanja zahtjeva) izvješćuje ispitanika:**

- o razlozima zbog kojih nije postupio
- o mogućnosti podnošenja pritužbe nadzornom tijelu i traženja pravnog lijeka

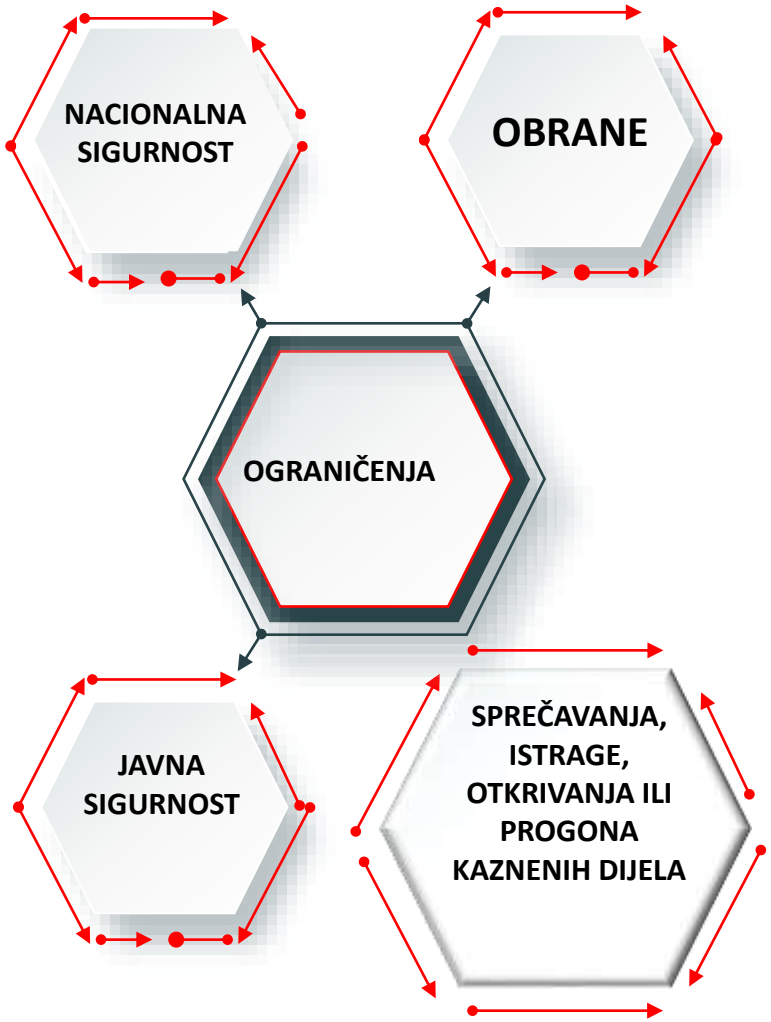
Voditelj obrade može:

→ Naplatiti razumnu naknadu

→ Odbiti postupiti po zahtjevu (*teret dokaza očigledne neutemeljenosti ili pretjeranosti zahtjeva je na voditelju obrade)*

## OGRANIČENJA
## (čl 23. Opće uredbe)

**Pravo na zaštitu osobnih podataka NIJE APSOLUTNO!**



# INTERNI AKTI

- 1. Stvaranje evidencija aktivnosti obrade
- 2. Izjava o povjerljivosti
- 3. Politika privatnosti
- 4. Pravilnik o zaštiti osobnih podataka
- 5. Ugovor sa izvršiteljem (ako je primjenjivo)
- Uputno:
- Pravilnik o informacijskoj sigurnosti
- Pravilnik o video nadzoru

# Evidencije aktivnosti obrade - NOVO

Opća uredba o zaštiti podataka **ne propisuje obvezu dostave evidencija o zbirkama osobnih podataka u Agenciju (Središnji registar)** te slijedom navedenog prestaje obveza voditelja obrade na dostavu evidencija zbirki osobnih podatka radi registracije u Središnji registar

Voditelji obrade osobnih podataka kao i izvršitelji obrade osobnih podataka imaju obvezu **voditi evidenciju aktivnosti obrade** pod uvjetima iz **čl.30 Opće uredbe o zaštiti podataka**

# Evidencije aktivnosti obrade

- Navedene obveze iz st.1 i 2. čl. 30 ne primjenjuju se na poduzeća ili organizaciju u kojoj je zaposleno **manje od 250 osoba**, osim:

  - ako će obrada koju provodi vjerojatno prouzročiti **visok rizik** za prava i slobode ispitanika
  - ako obrada **nije povremena**
  - ako obrada uključuje **posebne kategorije podataka**
  - ako je riječ o osobnim podacima u vezi s **kaznenim osudama i kažnjivim djelima**

**PREPORUKA DA SE USPRKOS IZNIMKAMA EVIDENCIJA NAPRAVI**

# Evidencije aktivnosti obrade - NOVO

- EVIDENCIJE AKTIVNOSTI OBRADE NE SADRŽE OSOBNE PODATKE

- Opća uredba ne propisuje poseban obrazac evidencije aktivnosti obrade

- Evidencije aktivnosti obrade pomaže u praćenju usklađenosti sa Općom uredbom o zaštiti podataka te mora biti u pisanom obliku, uključujući elektronički oblik

- Evidencije aktivnosti obrade ne dostavlja se nadzornom tijelu (Agenciji za zaštitu osobnih podataka), nadzornom tijelu na uvid prilikom obavljanja nadzornih aktivnosti

# Evidencije aktivnosti obrade

**Svaki voditelj obrade i predstavnik voditelja obrade vodi evidenciju aktivnosti obrade za koje je odgovoran.**

Ta evidencija sadržava sve sljedeće informacije (čl.30. st 1 Opće uredbe):

**1. ime i kontaktne podatke voditelja obrade**, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka

**2. svrhe obrade**

**3. opis kategorija** ispitanika i kategorija osobnih podataka

4. **kategorije primateljâ** kojima su osobni podaci otkriveni ili će im biti otkriven

5. **prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju,**

6. **predviđene rokove za brisanje** različitih kategorija podataka

7. **opći opis tehničkih i organizacijskih sigurnosnih mjera**

# Evidencije aktivnosti obrade – IZVRŠITELJ OBRADE

- **Svaki izvršitelj obrade i predstavnik izvršitelja obrade vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju za voditelja obrade.**

- Evidencija sadržava (čl.30 st.2):

  - **ime i kontaktne podatke** jednog ili više izvršitelja obrade i svakog voditelja obrade u čije ime izvršitelj obrade djeluje
  - **kategorije obrade** koje se obavljaju u ime svakog voditelja obrade
  - **prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju**, uključujući identificiranje te treće zemlje ili međunarodne organizacije te dokumentaciju o odgovarajućim zaštitnim mjerama
  - **opći opis tehničkih i organizacijskih sigurnosnih mjera**

# Uloga službenika vezano za vođenje evidencija

- Voditelj ili izvršitelj obrade, a NE službenik za zaštitu podataka, dužan je voditi evidenciju postupaka obrade

  - voditelj ili izvršitelj obrade ***može službeniku povjeriti zadaću vođenja evidencije postupaka obrade***

- Takva evidencija bi se trebala smatrati jednim od alata koji službeniku omogućuju obavljanje njegovih zadaća → praćenje usklađenosti, obavješćivanja i savjetovanja voditelja ili izvršitelja obrade i dr.

- Evidencija aktivnosti obrade - obrazac: https://azop.hr/wp-content/uploads/2023/07/ARC-obrazac-Evidencija-aktivnosti-obrade.xlsx

# PRIMJER1: EVIDENCIJA O ZAPOSLENICIMA

- **1. Naziv obrade: Evidencija podataka o zaposlenicima**
- **Kategorija ispitanika: Zaposlenici**
- **Svrha obrade: Vođenje evidencije o zaposlenicima**
- **Pravna osnova za obradu (čl.6.st1.):** Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c))
  Zakon o radu (NN 93/2014, 127/2017, 98/2019,Pravilnik o sadržaju i načinu vođenja evidencije o radnicima (NN 32/15, 97/15)
- **Kategorije osobnih podataka koje se obrađuju:** identifikacijski podaci (ime, prezime, oib, datum rođenja, spol, prebivalište, boravište, državljanstvo)
  podaci o obrazovanje, podaci o radnom stažu
- **Kategorije primatelja:** HZZO, HZMO, Porezna uprava
- **Rokovi brisanja (čuvanja):** Trajno (Članak 5. Pravilnik o sadržaju i načinu vođenja evidencije o radnicima NN 73/2017)
- **IT servis ili fizičko mjesto pohrane:** mapa u zaključanom ormaru u uredu vlasnika poduzeća; mapa pod nazivom zaposlenici u ERP-u, zaštićena šifrom
- **Opis poduzetih tehničkih i organizacijskih mjera:** Politika privatnosti, Pravilnik o zaštiti podataka, izjava o povjerljivosti, backup programa, antivirusni programi, evidencija pristupa osobnim podacima (logovi), edukacija zaposlenika na temu zaštite podataka, enkripcija, korištenje korisničkih imena i snažnih lozinki za pristup računalima i računalnoj opremi, antivirusni programi, redovito izrađivanje sigurnosnih kopija podataka. Papirnata dokumentacija koja sadrži osobne podatke nalazi se u zaključanom ormariću u zaključanoj prostoriji.

# PRIMJER2: VIDEOZAPISI POSJETITELJA OBJEKTA NA ADRESI

| | | |
|---|---|---|
| **Voditelj obrade:** | A d.o.o. | |
| **Kategorija ispitanika i osobnih podataka:** | Posjetitelji poslovnice I zaposlenici | |
| **Svrha:** | zaštita ljudi i imovine | |
| **Pravna osnova za obradu:** legitimni interes | **Rok za brisanje:** 6 mjeseci | |
| | | |

| | |
|---|---|
| **Izvršitelj obrade:** | B d.o.o. |
| **Vrsta obrade:** videonadzor u svrhu zaštite osoba i imovine objekta na adresi _____ | |
| **Prijenos:** - | **Teh. i org. Mjere:** Pravilnik o videonadzoru, edukacija zaposlenika, Ugovor sa izvršiteljem obrade, Izjave o povjerljivosti |

# IZJAVA O POVJERLJIVOSTI

- ZAGLAVLJE TVRTKE, MEMORANDUM

- **IZJAVA O POVJERLJIVOSTI**
- Ovom izjavom obvezujem se da ću sukladno propisima koji uređuju područje zaštite osobnih podataka, Uredbom (EU) 2016/679 europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka, čuvati povjerljivost svih osobnih podataka kojima imam pravo i ovlast pristupa a koji se nalaze u sustavima pohrane koje vodi tijelo/društvo u kojem sam zaposlen/a te da ću iste osobne podatke koristiti isključivo u točno određenu (propisanu) svrhu.

- Također se obvezujem da osobne podatke kojima imam pravo i ovlast pristupa neću dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnima trećim (neovlaštenim) osobama, te se obvezujem da ću povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima.

- Upoznat/a sam da bilo kakvo neovlašteno raspolaganje osobnim podacima kojima imam pravo pristupa  u svojem radu predstavlja povredu radne obveze.

- Datum: _____
- Ime i prezime: _____
- Potpis: _____

Izjava o povjerljivosti - obrazac: https://azop.hr/wp-content/uploads/2020/12/6-izjava_o_povjerljivosti_obrazac-1.docx

# POLITIKA PRIVATNOSTI

**POLITIKA PRIVATNOSTI (ZA WEB)**

- **VODITELJ OBRADE – NAZIV I KONTAKT**
- **PODACI O SLUŽBENIKU ZA ZAŠTITU PODATAKA**
- **SVRHA I PRAVNI TEMELJ ZA OBRADU OSOBNIH PODATAKA**
- **OBRADA OSOBNIH PODATAKA PUTEM VIDEO NADZORA**
- **KORIŠTENJE KOLAČIĆA**
- **PRAVA ISPITANIKA**
- - Pravo na pristup osobnim podacima
- - Pravo na ispravak osobnih podataka
- - Pravo na brisanje
- - Pravo na ograničavanje obrade
- - Pravo na prigovor
- - Davanje na korištenje osobnih podataka
- - Sigurnost osobnih podataka
- **KONTAKT ZA OSTVARIVANJE PRAVA**
- **ROKOVI ČUVANJA OSOBNIH PODATAKA**
- **POSTOJANJE AUTOMATIZIRANOG DONOŠENJA ODLUKA UKLJUČUJUĆI I IZRADU PROFILA**

Politika privatnosti - obrazac: https://azop.hr/wp-content/uploads/2023/06/politika-privatnosti_obrazac.docx

# UGOVOR SA IZVRŠITELJEM OBRADE

- **provođenje obrade od strane izvršitelja obrade trebalo bi biti uređeno ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice koji izvršitelja obrade obvezuje prema voditelju obrade (ČL.28. Opće uredbe)**
- **Voditelj obrade trebao bi angažirati samo izvršitelja obrade koji u dovoljnoj mjeri jamći sigurnost osobnih podataka**
- **UGOVOR SE SASTOJI** → predmet i trajanje obrade, priroda i svrhe obrade, vrsta osobnih podataka te kategorije ispitanika, uzimajući u obzir posebne zadaće i odgovornosti izvršitelja obrade u kontekstu obrade koju treba provesti te rizika za prava i slobode ispitanika
- OPREZ!! Potrebno regulirati pitanje što sa podacima nakon raskida ugovora.

Predložak ugovora voditelj-izvršitelj obrade: https://azop.hr/wp-content/uploads/2023/03/Ugovor-o-obradi-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-prema-clanku-28-OUZP-template.docx

# 3. PROCJENA RIZIKA I PROVOĐENJE PROCJENE UČINKA NA ZAŠTITU PODATAKA

- Dužnost je voditelja 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 dužnost **“provesti odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom”**

# PROCJENJIVANJE RIZIKA

- DPO također: pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade
- GDPR izrijekom ne zahtijeva uključenost DPO-a u bilo koju opću procjenu rizika: uredba propisuje takvo uključivanje DPO-a samo vezano za dublju Procjenu učinka na zaštitu podataka
- Međutim, u praksi bilo bi uputno uključiti DPO-a također i u ovu općenitiju procjenu rizika

- Valjana procjena rizika uključuje 4 koraka:

- 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)

# Što nakon procjene?

- DPO bi trebao:
- 1. dati savjet relevantnoj odgovornoj osobi ili osobama o tim rizicima
- 2. predložiti ublažavanje rizika ili alternativni postupak
- 3. voditi cjelovite evidencije o svim procjenama rizika i savjetima (čime se dokazuje usklađenost)
- 4. ako je „visok rizik” za prava i slobode pojedinaca, treba savjetovati voditelja obrade da je potrebna **cjelovita Procjena učinka na zaštitu podataka** (DPIA)

# PROVOĐENJE PROCJENE UČINKA NA ZAŠTITU PODATAKA (DPIA)

Procjena učinka na zaštitu osobnih podataka propisana je člankom 35. Opće uredbe - odnosi se na vjerojatni visoki rizik „za prava i slobode pojedinaca”

→ Procjena učinka na zaštitu podataka potrebna je barem u sljedećim slučajevima:

- sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima, uključujući izradu profila;
- opsežne obrade osjetljivih podataka;
- sustavnog praćenja javnog područja u velikoj mjeri

# Kriteriji koje treba uzet u obzir

1. Procjena ili bodovanje
2. Automatizirano donošenje odluka s pravnim ili sličnim značajnim učinkom
3. Sustavno praćenje
4. Osjetljivi podaci ili podaci iznimno osobne prirode
5. Obrada podataka u velikoj mjeri
6. Uparivanje ili spajanje baza podataka
7. Podaci koji se tiču osjetljivih pojedinaca
8. Inovativno korištenje novih tehnoloških ili organizacijskih rješenja
9. Kada obrada „*sprječava ispitanike u ostvarenju nekog prava ili korištenju usluge ili ugovora*”

Procjena učinka na zaštitu podataka - obrazac: https://azop.hr/wp-content/uploads/2020/12/7-DPIA-obrazac_procjena_ucinka-1.docx

| Primjeri obrade | Mogući relevantni kriteriji | Vjerojatnost da se zahtijeva DPIA |
|---|---|---|
| Bolnica koja obrađuje genetičke i zdravstvene podatke svojih pacijenata (bolnički informacijski sustav). | Osjetljivi podaci nadasve osobne prirode. - Podaci koji se tiču osjetljivih ispitanika. - Podaci obrađeni u velikoj mjeri. | da |
| Korištenje sustava kamera radi praćenja vozačkog ponašanja na autocestama. Voditelj obrade zamišlja korištenje inteligentnog sustava video analize da bi izdvojio automobile i automatski prepoznao registracijske pločice. | Sustavno praćenje. - Inovativno korištenje ili primjena tehnoloških ili organizacijskih rješenja | da |
| Trgovačko društvo sustavno nadzire aktivnosti svojih zaposlenika, uključujući praćenje radnih stanica zaposlenika, aktivnosti na mreži itd. | Sustavno praćenje. - Podaci koji se tiču osjetljivih ispitanika | da |
| Prikupljanje podataka javnih društvenih medija za generiranje profila. | Procjena ili bodovanje. - Podaci se obrađuju u velikoj mjeri. - Uparivanje ili kombiniranje skupova podataka. - Osjetljivi podaci nadasve osobne prirode | da |
| Institucija stvara kreditno bodovanje na nacionalnoj razini ili bazu podataka pronevjera. | Procjena ili bodovanje. - Automatizirano donošenje odluka s pravnim ili sličnim značajnim učinkom. - Sprječava ispitanika od ostvarenja nekog prava ili korištenja usluge ili ugovora. - Osjetljivi podaci ili podaci nadasve osobne prirode | da |
| Pohrana radi 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 | da |
| Obrada “osobnih podataka pacijenata ili klijenata pojedinih liječnika, drugih zdravstvenih djelatnika ili odvjetnika” | Osjetljivi podaci ili podaci nadasve 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 jednostavne načine odjave | Podaci obrađeni u velikoj mjeri | ne |
| Mrežne stranice za elektroničku trgovinu prikazuju oglase za starinske (vintage) auto-dijelove, što uključuje ograničeno profiliranje na temelju | Procjena ili bodovanje. | ne |

# Primjeri kada treba provesti DPIA a kada ne treba

**Potrebna je procjena učinka na zaštitu podataka**
Banka detaljno provjerava svoje klijente u odnosu na kreditnu referentnu bazu podataka; bolnica koja će početi upotrebljavati novu bazu zdravstvenih informacija sa zdravstvenim podacima pacijenata, autobusni prijevoznik koji će početi upotrebljavati videokamere u autobusu kako bi nadzirao ponašanje vozača i putnika.

**Procjena učinka na zaštitu podataka nije potrebna**
Liječnik u zajednici obrađuje osobne podatke svojih pacijenata. U tom slučaju nema potrebe za procjenom učinka na zaštitu podataka jer liječnici u zajednici ne provode opsežne obrade u slučajevima kad je broj pacijenata ograničen.

# POPIS AZOP-A O VRSTAMA POSTUPAKA OBRADE KOJE PODLIJEŽU ZAHTJEVU ZA DPIA

- ODLUKA o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka
- Donesena u skladu s člankom 35. stavkom 4. Opće uredbe o zaštiti podataka

Ravnatelj Agencije za zaštitu osobnih podataka donosi

**ODLUKU**

**o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka**

**I.**

Pored slučajeva predviđenih člankom 35. stavkom 3. Opće uredbe o zaštiti podataka, uzimajući u obzir izuzetak predviđen u članku 35. stavku 10. Opće uredbe o zaštiti podataka, provedba procjene učinka na zaštitu osobnih podataka obvezna je kod obrade osobnih podataka u sljedećim slučajevima:

1) Obrada osobnih podataka radi sustavnog i opsežnog profiliranja ili automatiziranog odlučivanja kako bi se donijeli zaključci koji u značajnoj mjeri utječu ili mogu utjecati na pojedinca i/ili više osoba ili koji služe kao pomoć u donošenju odluka o nečijem pristupu nekoj usluzi ili servisu ili pogodnosti (npr. kao što je obrada osobnih podataka odnosnih na ekonomski ili financijski status, zdravlje, osobne preferencije, interese, pouzdanost, ponašanje, podatke o lokaciji i dr.);
2) Obrada posebnih kategorija osobnih podataka u svrhu profiliranja ili automatiziranog odlučivanja;
3) Obrada osobnih podataka djece u svrhu profiliranja ili automatiziranog odlučivanja ili za marketinške svrhe, ili za izravnu ponudu usluga namijenjenu njima;
4) Obrada osobnih podatka prikupljenih od trećih strana koji se uzimaju u obzir za donošenje odluke vezane za sklapanje, raskidanje, odbijanje ili produženje ugovora o pružanju usluga fizičkim osobama;
5) Obrada posebnih kategorija osobnih podataka ili osobnih podataka o kaznenoj ili prekršajnoj odgovornosti u velikom opsegu;
6) Obrada osobnih podataka korištenjem sustavnog nadzora javno dostupnih mjesta u velikom opsegu;
7) Uporaba novih tehnologija ili tehnoloških rješenja za obradu osobnih podatka ili sa mogućnošću obrade osobnih podataka (npr. primjena „interneta stvari", poput pametnih televizora, pametnih kućanskih aparata, komunikacijski povezanih igračaka, sustava „pametni gradovi", pametnih mjerača energije, itd.) koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih osoba;
8) Obrada biometrijskih podataka kad je ispunjen bar još jedan kriterij iz Smjernica o procjeni učinka na zaštitu podataka (WP 248 rev. 01) koji služe za procjenu hoće li određeni postupci obrade vjerojatno prouzročiti visok rizik za prava i slobode ispitanika;
9) Obrada genetskih podataka kad je ispunjen bar još jedan kriterij iz Smjernica o procjeni učinka na zaštitu podataka (WP 248 rev. 01) koji služe za procjenu hoće li određeni postupci obrade vjerojatno prouzročiti visok rizik za prava i slobode ispitanika;
10) Obrada osobnih podataka povezivanjem, usporedbom ili provjerom podudarnosti iz više izvora;
11) Obrada osobnih podataka na način koji uključuje praćenje lokacije ili ponašanja pojedinca u slučaju sustavne obrade komunikacijskih podataka (metapodaci) nastalih uporabom telefona, interneta ili drugih komunikacijskih kanala, kao što je GSM, GPS, Wi Fi, praćenje ili obrada podataka o lokaciji;
12) Obrada osobnih podataka korištenjem uređaja i tehnologija kod kojih incidentni događaj može ugroziti zdravlje pojedinca ili više osoba;
13) Obrada osobnih podataka zaposlenika uporabom aplikacija ili sustava za praćenje (npr. kao što je obrada osobnih podatka za praćenje rada, kretanja, komunikacije i sl.).

# SURADNJA SA NADZORNIM TIJELOM

- *<u>DPO DJELUJE KAO</u>*:
- KONTAKTNA TOČKA radi lakšeg pristupa dokumentima i informacijama radi lakšeg obavljanja zadaća AZOP-a
- ODGOVARA NA ZAHTJEVE AZOP-a i inicira suradnju na zahtjev tijela ili na vlastitu inicijativu
- SAVJETODAVNA FUNKCIJA - kao sastavni dio organizacije u kojoj je zaposlen – zadužen je za osiguravanje sukladnosti iznutra te može intervenirati u ranom stadiju na način da se savjetuje sa AZOP-om i pruži savjete voditelju
- PROVEDBENA FUNKCIJA – trebali bi pokušati istražiti i riješiti pritužbe na lokalnoj razini prije slanja AZOP-u
- MJERENJE UČINKOVITOSTI – smatra se korisnim alatom za procjenu napretka, poticanje na razvoj vlastitih kriterija dobrog nadzora

# Kvalitetna priprema za nadzorne aktivnosti

# Pitanja za samoprocjenu

- ✓ **Čiji i koji osobni podaci se obrađuju i pohranjuju?**
- ✓ **Koje sustave pohrane imate?**
- ✓ **Koji Vam je pravni temelj za obradu podataka?**
- ✓ **Znate li  u koju svrhu  prikupljate i pohranjujete osobne podatke?**
- ✓ **Tko ima pravo pristupa tim podacima? Tko ih koristi?**
- ✓ **Da li je nužno prikupljanje tih osobnih podataka?**
- ✓ **Da li se podaci iznose u treće zemlje? Zakonitost takvog iznošenja?**
- ✓ **Da li se ti podaci prosljeđuju trećim osobama te temeljem koje zakonske osnove?**
- ✓ **Koji je vremenski rok čuvanja tih podataka i što se s njima događa nakon toga?**

- ✓ **Jesu li osobni podaci točni i ažurirani?**
- ✓ **Gdje se podaci spremaju i u kojem obliku (digitalnom/paprinatom)?**
- ✓ **Prikupljate li „osjetljive podatke”?**
- ✓ **Koji propisi reguliraju korištenje osobnih podataka?**
- ✓ **Vodite li računa o sigurnosti osobnih podataka?**
- ✓ **Jesu li Vaši zaposlenici svjesni važnosti zaštite osobnih podataka? Izjava o povjerljivosti?**
- ✓ **Da li su tehničke mjere u skladu s člankom 32. Uredbe i drugim povezanim člancima i posebnim propisima?**

PREPORUKA AZOP-a: VODIČI I OBRASCI ZA USKLAĐIVANJE S OPĆOM UREDBOM O ZAŠTITI PODATAKA (izrađeni u suradnji s irskim nadzornim tijelom za zaštitu podataka i namijenjeni prvenstveno mikro, malim i srednjim poduzetnicima, ali primjenjivi na sve voditelje/izvršitelje obrade):

https://arc-rec-project.eu/edukativni-materijali/

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Co-funded by the European Union

# HVALA NA POZORNOSTI