P/

REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU
OSOBNIH PODATAKA

KLASA:
URBROJ:
Zagreb,

Agencija za zaštitu osobnih podataka (OIB: 28454963989), na temelju članka 57. stavka 1., članka 58. stavka 1. i 2. točke (i) i članka 83. 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) SL EU L119, članaka 36., 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18), a postupajući po službenoj dužnosti protiv društva X, OIB: __, u postupku zaštite osobnih podataka, donosi sljedeće:

R J E Š E NJ E

1. Utvrđuje se da je nepoduzimanjem odgovarajućih organizacijskih i tehničkih mjera sigurnosti obrade osobnih podataka od strane društva X kao izvršitelja obrade za društvo Y, došlo do kršenja sigurnosti obrade koje je dovelo do neovlaštenog otkrivanja osobnih podataka ispitanika, odnosno do kršenja odredbi članka 32. stavka 1. točke b) i d) te stavka 2. Opće uredbe o zaštiti podataka.

2. Za kršenje opisano u točki 1. izreke ovog rješenja, u skladu s odredbama članka 83. stavka 2. i stavka 4. točke a) Opće uredbe o zaštiti podataka, izriče se društvu X upravna novčana kazna u iznosu od:

17.500,00 Eura
(slovima: sedamnaesttisućapetstoeura)

3. Društvo X , dužno je platiti izrečenu upravnu novčanu kaznu u korist državnog proračuna u roku od 15 dana od dana pravomoćnosti ovog rješenja u korist računa broj: **HR1210010051863000160, model HR64 i poziv na broj odobrenja _** s naznakom - “upravne novčane kazne koje izriče AZOP”.
4. Ukoliko društvo X, u roku od 15 dana od pravomoćnosti ovog rješenja ne plati izrečenu upravnu novčanu kaznu, Agencija će sukladno članku 46. stavku 2. Zakona o provedbi Opće uredbe o zaštiti podataka obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području sjedište navedenog društva radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza.

5. Društvo X je dužno u roku od 15 dana od izvršene uplate dostaviti dokaz o uplati na uvid ovoj Agenciji.

O b r a z l o ž e n j e

I. UTVRĐENJE POVREDE

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija) zaprimila je dana 21. veljače 2024. Izvješće o povredi osobnih podataka prema čl. 33 Opće uredbe o zaštiti podataka od 21. veljače 2024. voditelja obrade Y štedionice, kojim se Agenciju izvješćuje da je Štedionica tijekom 19. i 20. veljače 2024. u nekoliko navrata i telefonskim putem i e-mailom zaprimila prijave klijenata koji su na svojoj kućnoj adresi zaprimili neispravne Izvode s računa, odnosno Izvode s računa koji djelomično sadrže podatke s Izvoda i drugih klijenata Štedionice, a ne samo ciljanih primatelja, da je riječ o Izvodima koji su kuvertirani na temelju predefiniranih „jobova" i poslani 16. veljače 2024. godine posredstvom vanjskog suradnika Štedionice – X a u okviru slanja redovnih godišnjih izvoda, da su kategorije ispitanika koji su zahvaćeni ovom povredom klijenti Štedionice koji su sudionici u kreditu za međufinanciranje kredita stambene štednje (K100) a povreda se potencijalno odnosi na 1204 klijenata, sukladno spornom „jobu" koji je sadržavao 1204 pošiljke.
Dalje se navodi da su izvodi kuvertirani i poslani 16. veljače 2024. a najizglednije je da su iste klijenti počeli zaprimati 19. veljače 2024. kada je u Štedionici zaprimljena prva prijava klijenta, da se podaci na koje se povreda odnosi su svi podaci koji su sadržani na Izvodu s računa (identifikacijski podaci - ime, prezime; kontakt podaci – adresa; podatak o broju ugovora o kreditu/štednji vezanoj uz kredit; podaci o prometu po računu), da je do trenutka prijave AZOP-u, Štedionica od strane klijenata zaprimila 11 prijava krivo dostavljenih Izvoda.

Isto se navodi da je Štedionica 20. veljače 2024. uputila upit Xza provjeru postojanja greške u slanju prvog dijela Izvoda te zatražila obustavu daljnjeg slanja Izvoda dok se ne utvrde okolnosti slanja i eventualnog propusta, da je 21. veljače 2024. X potvrdio da je došlo „do greške" u obradi mape koja je sadržavala 1204 pošiljke te da je Štedionica od X zatražila detaljno pisano očitovanje o nastalom propustu.

Dana 1. ožujka 2024. Agencija je od voditelja obrade Y zaprimila dopunu Izvješća od 21. veljače 2024., u kojem se između ostalog navodi da čekaju detaljnije očitovanje društva X kao izvršitelja obrade o nastaloj povredi, ali da je društvo X u vidu otvorene suradnje dostavilo informacije o tipu greške prema kojem je društvo Y provelo rekonstrukciju te je na temelju iste utvrđeno da je riječ o 1204 kreditna predmeta koji su se na tiskarskom stroju ispisivali iz pet (5) „jobova", no da se povreda odnosi na tarife za međufinanciranje kredita, a ne samo na K100 tarifu kako je inicijalno navedeno, a da je ukupan broj ispitanika na koji se odnosi povreda 1654 budući da je jedan kreditni predmet/Izvod u sebi može sadržavati informacije kako nositelja kredita, tako i članova obitelji koji su povezani s tim kreditom.

Također, navodi se da su, uzevši u obzir novoutvrđene okolnosti, svi ispitanici koji su pogođeni povredom podijeljeni na tri (3) osnovne kategorije, ovisno o vrsti povrede odnosne na njih, kako slijedi:

- klijenti čiji su Izvodi s računa poslani drugim klijentima, no isti istovremeno nisu primili nijedan Izvod (niti svoj niti tuđi),
- klijenti koji su uz Izvod koji glasi na njihovo ime zaprimili i Izvode s računa drugih klijenata (dakle, njihovi podaci nisu otkriveni trećim stranama) te,
- klijenti čiji su Izvodi s računa poslanim drugim klijentima, a istovremeno su i sami zaprimili tuđe.

Isto tako, navodi se da je društvo Y nakon točne identifikacije klijenata prema prethodno definiranoj vrsti povrede pripremilo službene obavijesti kako bi svakog pojedinog klijenta izravno obavijestila o povredi i situaciji primjenjivoj na njega te dala uputu za daljnje postupanje. Konkretno, dopisima se, uz očekivano informiranje o povredi sukladno pozitivnoj praksi, klijente upućuje na uništavanje ili povrat dokumentacije za koju nisu bili namjeravani i ovlašteni primatelj, odnosno upućuje isprika i pojašnjavaju okolnosti povrede u slučaju da nisu dobili tuđe osobne podatke. Također, navodi se da se predmetni dopisi planiraju poslati na kućnu adresu svih „pogođenih“ ispitanika, nakon čega će se klijentima koji su inicijalno trebali dobiti redovno godišnje Izvode s računa (nositelji kredita) ponoviti slanje istih.

Agencija je dopisom KLASA: __, URBROJ: __ od 4. ožujka 2024. od društva Y, zatražila očitovanje i dostavu evidencija aktivnosti obrade uspostavljenih kod voditelja obrade Y, ugovore o suradnji između voditelja obrade Y i izvršitelja obrade X, preslike akata voditelja obrade, Y odnosnih na uređenje obrade osobnih podataka unutar istog, preslike akata voditelja obrade Y odnosnih na sigurnost obrade osobnih podataka, odnosno tehničkih i organizacijskih mjera koje provodi voditelj obrade, posebice vezano uz informacijsku sigurnost, opisati na koji način i u kojem obliku voditelj obrade Y dostavlja izvršitelju obrade X datoteke/datoteku koja sadrži osobne podatke ispitanika i koja se koristi za provedbu aktivnosti ispisivanja i slanja Izvoda računa na način opisan u predmetnoj povredi te navesti tko je temeljem ugovorenog odnosa između voditelja obrade Y i izvršitelja obrade X bio zadužen za organizacijske i tehničke mjere zaštite obrade osobnih podataka ispitanika, a koje su imale za cilj prevenciju pojavnost predmetne povrede.

Agencija je dopisom KLASA:__, URBROJ: __ od 5. ožujka 2024. od društva X, kao izvršitelja obrade zatražila očitovanje i dostavu detaljnog opisa okolnosti predmetne povrede od 16. veljače 2024., da navede zbog čega je došlo do greške u programu, priloži preslike greške u „kodu“ programa i učinjene ispravke te navede vremenski period u kojem je greška bila prisutna, zatim da navede naziv programskog rješenja koje koristi društvo X za obradu osobnih podataka dostavljenih od strane Y i pripremu istih za tisak, da opiše na koji način i u kojem obliku X zaprima od Y datoteke/datoteku koja sadrži osobne podatke ispitanika i koja se koristi za provedbu aktivnosti ispisivanja i slanja Izvoda s računa na način opisan u predmetnoj povredi, da dostavi preslike ugovora sklopljenih između Y i X te navede organizacijske i tehničke mjere koje je društvo X poduzelo naknadno a koje imaju za cilj prevenciju pojavnosti iz predmetne povrede.

Dana 18. ožujka 2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane društva X kao izvršitelja obrade, u kojem se, između ostalog, navodi da su dana 15. veljače 2024. (14:16) zaprimili datoteke od voditelja obrade, društva Y, putem kriptiranog kanala (sftp), u pdf formatu, a dokumenti su sadržavali dodatni barkod za kuvertiranje, bez popratne statistike za kontrolu, a zahtjev za slanje pošiljaka na poštu je bio 16. veljače 2024. Nadalje, navodi se da su u obradu datoteka krenuli 16. veljače 2024. ujutro te da je u tijeku procesa kuvertiranja posla „MFIN Krediti“ 16. veljače 2024. oko 12,00 sati došlo do kvara/zastoja na stroju za kuvertiranje. Također, navodi se da kako bi ispunili zahtjev voditelja obrade za predaju pošiljki na poštu 16. veljače 2024., a čije vozilo dolazi u prikup pošiljki u 14,00 sati, odlučili su radnju kuvertiranja obaviti na drugom stroju za kuvertiranje. Isto tako, navodi se da je na poštu predano 1205 komada kuverti, a količina je utvrđena na temelju „brojača“ na izlazu iz stroja za kuvertiranje. Nadalje, navodi se da je dana 20. veljače 2024., oko 15,00 sati dojavljeno od strane voditelja obrade kako im se javlja više komitenata koji su unutar kuverte primili svoj i tuđi izvod. Također, navodi se da je izvršeno prikupljanje logova obrade iz strojeva, sustava za praćenje i ostalih informacija unutar procesa obrade (izjave zaposlenika), izvršeno je uspoređivanje sa zaprimljenim datotekama te je utvrđeno da je ispravan broj kuverti bio 1204 komada, a ne 1205 komada koliko je predano na poštu.
Dalje se navodi da je ovaj događaj obrađen sukladno procedurama u sklopu sustava upravljanja informacijskom sigurnošću kao sigurnosni incident te je utvrđeno da je kod prebacivanja posla na drugi stroj za kuvertiranje i učitavanje konfiguracije postavki stroja, operater na kuvertirki nepažnjom učitao pogrešni modul, što je rezultiralo pogrešnim čitanjem barkoda na dokumentima i pogrešnim grupiranjem, odnosno insertiranjem dokumenata u kuverte, da jedna pošiljka odnosno kuverta sadrži više listova izvoda, a zbog pogrešnog čitanja barkoda na dokumentima, zadnji list izvoda je insertiran kao prvi list u novu kuvertu zajedno sa izvodima slijedećeg kredita, odnosno ugovora i tako nizom do kraja, te da je u žurbi operater na kuvertirki propustio izvršiti uobičajenu kontrolu ispravnosti kuvertiranja koja se radi kod prebacivanja posla na drugi stroj.

Isto tako, navodi se da je izvršena edukacija zaposlenika u procesu obrade (ispis i kuvertiranje) radi obnove znanja o pravilnom načinu upravljanja strojevima za kuvertiranje te radi podizanja svijesti o osjetljivosti procesa obrade osobnih podataka i važnosti konstantnog nadzora i kontrole procesa obrade dokumenata (ispis, kuvertiranje). Nadalje, navodi se da je radi poboljšanja procesa uvedena dodatna kontrola kod kuvertiranja u smislu nasumičnog fizičkog pregleda sadržaja kuverte, a nakon učitavanja strojnog moda za upravljanje. Također, navodi se da je u tijeku utvrđivanje Protokola o razmjeni i kontroli datoteka za produkciju dokumenta, kao priloga Ugovoru o produkciji dokumenata, a tim protokolom ugovorne strane će definirati pravila i postupke u cilju osiguranja sigurnog postupanja s osjetljivim i povjerljivim podacima u izvršenju usluge produkcije dokumenata te osiguranja točnosti ispisa i kuvertiranja personaliziranih dokumenata prema zaprimljenim podacima.
Očitovanju se prilaže preslika Ugovora o okvirima poslovne suradnje __ od 15.01.2019., preslika Sporazuma o zaštiti osobnih podataka br. __ od 15.01.2019., preslika Ugovora o produkciji dokumenata od 15.01.2019., preslika Aneksa ugovora o produkciji dokumenata od 04.11.2021., preslika Aneksa ugovora o produkciji dokumenata od 22.12.2023.

Uvidom u dostavljeni *Sporazum o zaštiti osobnih podataka br.* __ između Y kao voditelja obrade i X kao izvršitelja obrade, od 15.01.2019., navodi se u točki 6: *„Uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade definirane Ugovorom, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinca čiji se osobni podaci obrađuju ili mogu obrađivati, Izvršitelj se obvezuje provoditi odgovarajuće tehničke i organizacijske mjere u svrhu osiguranja, povjerljivosti, integriteta osobnih podataka te dokazivosti da se obrada osobnih podataka provodi u skladu sa svim propisima o zaštiti osobnih podataka i isključivo prema nalogu Voditelja, odnosno u skladu s pravima Izvršitelja koja proizlaze iz Ugovora.“*, a u točki 14: „*Izvršitelj je dužan bez odgode upozoriti Voditelja na sve okolnosti koje predstavljaju ili mogu predstavljati kršenje propisa o zaštiti osobnih podataka te poduzeti sve potrebne i moguće mjere sukladno nalogu Voditelja s ciljem izbjegavanja povrede osobnih podataka ispitanika, odnosno mjere umanjivanja mogućih štetnih posljedica ukoliko dođe do povrede osobnih podataka. Obavijest o mogućnosti povrede osobnih podataka i onu koja je već rezultirala povredom osobnih podataka, a koja obavezno sadržava, ali se ne ograničava na, informacije o svim okolnostima u kojima se utvrđuje povreda ili potencijalna povreda, kao i vrijeme saznanja iste te broj pogođenih ispitanika, Izvršitelj je dužan neodgodivo dostaviti na adresu elektroničke pošte __, na broj telefaksa __ s naznakom „DPO-hitno“ ili pozivom na broj telefona __.“*

Uvidom u dostavljeni *Ugovor o produkciji dokumenata* između X kao Izvršitelja i Y kao Naručitelja, u članku 6. navodi se: *„U cilju pružanja primjerene razine usluge, izvršitelj se obvezuje sljedeće:*

- *o svom trošku ponoviti uslugu ukoliko dođe do pogreške prilikom tiska, ispisa varijabilnih podataka ili kuvertiranja*
- *s krajnjom pažnjom i odgovornošću postupati sa svim materijalima koje dobiva od Naručitelja*
- *osigurati zaštitu zaprimljenih podataka kako u tehničkom pogledu, tako i od strane ljudskog faktora,*
- *osigurati točnost otisaka i kuvertiranja personaliziranih dokumenata prema zaprimljenim podacima,*
- *obavijestiti Naručitelja o svim činjenicama i promjenama okolnosti koje značajno utječu ili koje bi mogle značajno utjecati na ispunjenje ugovornih obveza,*
- *pri pružanju usluge u cijelosti postupati u skladu s važećim propisima Republike Hrvatske,*

u članku 13. se navodi: *„Izvršitelj je dužan kontinuirano provoditi kontrolu poslovnog procesa vezano za obavljanje poslova iz ovog ugovora, na način da provodi kontinuirani nadzor i da promptno detektira greške u ispisivanju i kuvertiranju dokumenata te ukoliko se greška utvrdi, da istu promptno otkloni. U obavljanju usluga koje su predmet ovog ugovora, Izvršitelj se obvezuje uspostaviti i održavati razinu zaštite povjerljivih informacija jednaku onoj kod Naručitelja. Po završetku konkretnog posla Izvršitelj se obvezuje vratiti Naručitelju sve medije, odnosno uništiti sve osobne podatke i informacije koje su razmijenjene temeljem ovog ugovora te Naručitelju dostaviti dokumentaciju kojom potvrđuje uništavanje navedenog. Izvršitelj je dužan u najkraćem roku obavijestiti Naručitelja u slučaju pojave sigurnosnog Incidenta koji na*

bilo koji način može utjecati na povjerljivost i cjelovitost odnosno za posljedicu imati kompromitaciju osobnih podataka klijenata Naručitelja. Dovršenjem posla iz ovog ugovora, ne prestaje obveza Izvršitelja na zaštitu tajnosti podataka, kao i odgovornost za nastalu štetu zbog povrede tajnosti. Izvršitelj je dužan dokumente, koji nisu podobni za slanje, uništiti kako ne bi mogli doći u posjed treće neovlaštene osobe".

Uvidom u dostavljeni *Aneks ugovora o produkciji dokumenata* između Y kao Pretplatnika i X kao Izvršitelja, u članku 2. *Sigurnost usluga* navodi se: „*Izvršitelj je dužan implementirati i redovito održavati minimalne tehničke i organizacijske sigurnosne mjere kako bi osigurao zadovoljavajuću razinu sigurnosti informacijskog sustava i podataka koji se obrađuju u kontekstu ovog Ugovora.*
Minimalne sigurnosne mjere potrebno je primijeniti minimalno na onim komponentama informacijskog sustava koje obrađuju podatke Naručitelja i koje su nužne za izvršenje odredbi ovog Ugovora, a poželjno na cijelom informacijskom sustavu. Minimalne sigurnosne mjere koje je potrebno implementirati i redovito održavati su: Politika sigurnosti informacijskog sustava, Primjereno upravljanje informacijskim sustavom, Klasifikacija informacija, Sustav za zaštitu od malicioznog softvera (antimalware zaštita), Snažna autentikacija, Upravljanje pravima pristupa sukladno poslovnoj potrebi, Sustav za centralizirano upravljanje log zapisima i sigurnosnim događajima, Segmentacija računalne mreže i filtriranje mrežnog prometa sukladno poslovnoj potrebi (vatrozidna zaštita), Periodička provjera ranjivosti informacijskog sustava, Redovita instalacija sigurnosnih zakrpi, Redovita izrada pričuvne pohrane (backup) i zaštita pričuvne kopije od uništenja /gubitka, Provođenje edukacije o podizanju svijesti o informacijskoj sigurnosti, Zaštita prijenosnih medija i mobilne računalne opreme, Fizička kontrola pristupa, Zaštita fizičkih lokacija i prostora, Enkripcija podataka u prijenosu i pohrani, Visoka raspoloživost (High availability), Upravljanje kontinuitetom poslovanja (Business Continuity Management), Uspostava pričuvne lokacije i procesa oporavka informacijskog sustava u slučaju katastrofe (Disaster Recovery)."

Dana 19. ožujka 2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane društva Y, kao voditelja obrade, u kojem se, između ostalog, dostavlja tražena dokumentacija: evidencije aktivnosti obrade koje društvo Y vodi kao voditelj obrade osobnih podataka (evidencije su kategorizirane po vrsti ispitanika čiji podaci su predmet obrade u poslovnim procesima), ugovornu dokumentaciju s X s pripadajućim aneksima i dodacima osnovnom Ugovoru, interne akte društva Y iz područja zaštite osobnih podataka, kao i iz drugih djelokruga rada, a koja se po svojoj prirodi djelomično dotiču zaštite privatnosti te interne akte društva Y iz područja informacijske sigurnosti.

Nadalje, u očitovanju društva Y, navodi se da se od 22. siječnja 2019. razmjena baza za ispis odvija preko kriptiranog dostavnog kanala, odnosno preko SFTP protokola s nestandardnim portom za spajanje, a razmjena korisničkog imena i zaporke te javnih ključeva za kriptiranje komunikacije provela se preko različitih komunikacijskih protokola. Također, navodi se da se slanje baze za ispis i kuvertiranje sastoji od jedne ili više ZIP datoteka koje sadrže .pdf dokumente za ispis/kuvertiranje, a koje se šalju društvu X, prethodno navedenim kanalom. Isto tako, navodi se da je ova dostava obavezno popraćena i s e-mail komunikacijom prema kontakt

osobi u društvu X s pojašnjenjem načina i vremena u kojem se dostavljeno treba ispisati, kuvertirati i otpremiti prema pošti.
Očitovanjem se dostavlja e-mail korespondencija vezana uz kreiranje dostavnog kanala datoteka za ispis (e-mailovi iz 2019. godine), kao i korespondencije (e-mailovi u razdoblju 09. siječnja 2024. - 16. veljače 2024.) koja se odvijala tijekom (primarno) veljače 2024. u okviru pripremnih radnji i dogovora oko slanja aktualnih izvoda s računa pri čijem slanju je, u konačnici došlo do propusta.

Također, navodi se da je u odnosu na zaduženja za organizacijske i tehničke mjere zaštite osobnih podataka klijenata/ispitanika, do sada je uobičajena praksa bila da se prije konačnog slanja izvoda radi test ispisa od strane društva Y, a u tom testu društvo Y priprema i društvu X šalje reprezentativne primjerke nekoliko grupa dopisa koje se potom ispisuju i vraćaju nazad u društvo Y na ručnu provjeru ispravnosti postupka. Nadalje, navodi se da se nakon uspješne provjere testnog seta, dostavljaju konačne (produkcijske) datoteke i pokreće se postupak ispisa, kuvertiranja i slanja. Sve izvode koji su bili jednostrani kuvertiralo je i slalo društvo X, dok se ostatak višestranih dopisa/izvoda i izvoda koji se odnose na kredite vraćalo u društvo Y na ručno kuvertiranje i slanje nakon što bi društvo X odradilo ispis.

Isto tako, navodi se da se ove godine odstupilo od dosadašnje prakse te je s društvom X dogovoreno ispisivanje, kuvertiranje i slanje svih izvoda (i višestranih), u koje svrhe je dogovoren novi način kuvertiranja koji uključuje DATAMATRIX barkod na listovima, a definicija kuvertiranja odrađena je prema specifikacijama društva X za 2D barkod za strojno pakiranje. Nadalje, navodi se da je društvo Y i u ovom slučaju, a posebice uzevši u obzir da se mijenja uobičajena procedura, nakon potvrde ispravnosti barkoda društvu X poslala testnu datoteku nakon čijeg ispisa i kuvertiranja je zatražila osobno preuzimanje testnih izvoda od strane djelatnika društva Y na lokaciji društva X (dostavljena e-korespondencija od 14. veljače 2024.). Također, navodi se da su predmetni izvodi (60 komada kuverti) dostavljeni u Središnji ured društva Y te je svaka pošiljka ručno otvorena kako bi se provjerila ispravnost njezinog sadržaja, odnosno je li dokumentacija ispravno kuvertirana. Nadalje, navodi se da je testom potvrđena ispravnost te se potom krenulo na dogovor oko ispisa i kuvertiranja produkcijske baze izvoda. Daljnji dogovor i dostava produkcijske baze uslijedila je 15. veljače 2024., s napomenom da se jedna od dvije dostavljene datoteke treba ispisati, kuvertirati i poslati s datumom 16. veljače, a druga 23. veljače 2024. Također, navodi se da je uz manja usklađivanja informacija oko obrade tih datoteka, djelatnik društva X na dan 16. veljače 2024. (dan koji je predviđen za produkciju) prvi put u e-mailu navodi potrebu za statistikom (specifikacijom) dostavljenih datoteka u svrhu kontrole podudarnosti broja „ulaznih“ i „izlaznih“ pošiljki. Isto tako, navodi se da budući da društvo Y ovom informacijom nije raspolagalo ni u jednom trenutku tijekom cijelog postupka dogovaranja novog procesa koji je trajao već mjesec i pol dana, produkcijske datoteke na sam dan predviđene produkcije nisu imale mogućnost naknadnog prebrojavanja, u kojem smislu je društvu X upućen i odgovor (s napomenom da će se ista pripremiti za ovakve buduće obrade) te je potvrđena daljnja obrada.

Društvo Y navodi kako mu ni u jednom trenutku, a niti tijekom cijelog postupka dogovaranja novog načina kuvertiranja od strane društva X nije skrenuta pozornost na neophodnost i važnost

te „statistike“. Također, navodi se da je društvo X na potvrdu društva Y nastavilo s daljnjom obradom bez ikakvog upozorenja na potencijalni propust koji može proizaći iz nedostatka te kontrole.

Nadalje, društvo Y navodi da prema ugovornoj definiciji, iz Aneksa Ugovora o produkciji dokumenata od 22.12.2023., prema čl. 2. Sigurnost usluga glasi: „Izvršitelj je dužan implementirati i redovito održavati minimalne tehničke i organizacijske sigurnosne mjere kako bi osigurao zadovoljavajuću razinu sigurnosti informacijskog sustava i podataka koji se obrađuju u kontekstu ovog Ugovora“. Nadalje, u Ugovoru o produkciji dokumenata od 15.01.2019. u čl. 5. stoje obveze Izvršitelja (društva X), prema kojima se, između ostalog, društvo X obvezuje: „…osigurati zaštitu zaprimljenih podataka kako u tehničkom pogledu, tako i od strane ljudskog faktora… i… obavijestiti Naručitelja o svim činjenicama i promjenama okolnosti koje značajno utječu ili koje bi mogle značajno utjecati na ispunjenje ugovornih obveza…“ Dodatno, navodi se u čl.13.: „Izvršitelj je dužan kontinuirano provoditi kontrolu poslovnog procesa vezano za obavljanje poslova iz ovog ugovora, na način da provodi kontinuirani nadzor i da promptno detektira greške u ispisivanju i kuvertiranju dokumenata, te ukoliko se greška utvrdi, da istu promptno otkloni.“ i „Izvršitelj je dužan u najkraćem roku obavijestiti Naručitelja u slučaju pojave sigurnosnog incidenta koji na bilo koji način može utjecati na povjerljivost i cjelovitost odnosno za posljedicu imati kompromitaciju osobnih podataka klijenata Naručitelja.“ Unatoč tome, u čl. 16. ovog Ugovora stoji i da će društvo Y „ davati Izvršitelju na raspolaganje sve dokumente i podatke koji su nužni za izvršenje usluge…“

Nadalje, društvo Y smatra da se na proces ispisa i kuvertiranja produkcijske baze izvoda nisu primijenile primjerene sigurnosne i kontrolne mjere od strane društva X, posebice uzevši u obzir činjenicu da je isto za povredu doznalo dojavom društva Y dana 20. veljače 2024. (dostavljena e-korespondencija) te da društvo X nije „detektiralo greške u ispisivanju i kuvertiranju dokumenata“, sukladno prethodno spomenutom čl. 13. niti je „osiguralo zaštitu zaprimljenih podataka kako u tehničkom pogledu, tako i od strane ljudskog faktora“, sukladno čl. 5. jer je povreda nastala ljudskom pogreškom unosa krivog koda u stroj za kuvertiranje na kojem nije provedeno novo testiranje (potreba za ponovnim unosom koda se pojavila jer je produkcijski stroj na kojem je test napravilo i društvo Y imao kvar te je društvo X daljnju obradu, bez ikakve obavijesti društvu Y, provelo na novom stroju bez ikakvog testiranja).

Također, navodi se da je društvo Y, nakon što je utvrdilo da je došlo do sigurnosnog incidenta koji je rezultirao povredom osobnih podataka klijenata e-mailom 20. veljače 2024. obavijestilo društvo X o dojavama koje je zaprimilo od klijenta te zatražilo hitnu provjeru pogreške kod slanja izvoda, uz napomenu o stopiranju daljnjeg slanja. Nadalje, navodi se da je u očitovanju od društva X navedeno da je riječ o 1204 pošiljke na kojima se dogodila greška te se potvrđuje da je riječ o 1204 kuverte koje su za društvo Y izvršene 16. veljače 2024. Također, navodi se da je društvo Y imalo online sastanak sa društvom X, a vezano uz navedeni događaj i situaciju. Po završetku sastanka, navodi se da je društvo Y zatražilo novo detaljnije očitovanje o pogrešci, na što je tek 26. veljače 2024. društvo X dostavilo e-mail s pojašnjenjem upisa krivog koda u stroj za kuvertiranje te primjerom greške kakvom je rezultirala ta ljudska pogreška. Isto tako, istog dana, 26. veljače 2024. službenik za zaštitu podataka društva Y uputio je društvu X putem

e-mail zahtjev za očitovanjem i specifikacijom vezano uz sve bitne okolnosti oko nastale povrede, a traženo očitovanje dostavljeno je 29. veljače 2024.

Nadalje, navodi se da je društvo Y u međuvremenu provelo rekonstrukciju nastale povrede na svojoj bazi podataka kako bi utvrdilo točan broj predviđenih pošiljaka te točan broj klijenta zahvaćenih povredom i identificirali te klijente u svrhu njihova obavještavanja. Na taj način utvrđeno je da se radi o 1204 pošiljke što je podudarno s informacijom dobivenom od društva X. Također, navodi se da je društvo Y zbog nedosljednosti i nerazumijevanja dodatnog očitovanja dostavljenog od strane društva X, zatražilo dostavu internog akta kojim su propisane i regulirane sigurnosne mjere i kontrole koje se provode prilikom ovakvih vrsta obrade podataka (ispis, kuvertiranje i slanje), a da dana 1. ožujka 2024. društvo X navodi da broj „ulaznih“ i „izlaznih“ pošiljki nije podudaran te da je ispisom datoteke društvo X imalo završno 1205 pošiljki (jednu više).
Isto tako, Y navodi da X do sada Štedionici nije dostavio interni akt o kontrolama koje se provode od strane Izvršitelja tijekom obrade podataka, dok se tijekom ponovnog online sastanka održanog 11. ožujka 2024., izjasnio da takvim dokumentom ne raspolažu, odnosno da kontrole koje provode proizlaze iz svakog pojedinačnog radnog naloga po kojem provode konkretnu obradu. Y zaključuje da društvo X možebitne kontrole provodi „ad hoc“ bez da je to i na koji način regulirano i propisano, što je u direktnoj suprotnosti ugovornih odredbi o sigurnosti na koje su se obvezali i koje bi trebale proizlaziti iz ISO/IEC 27001:2013 standarda.

Također, navodi se da se kao olakotna okolnost pojavila činjenica da dio klijenata koji su trebali biti „pogođeni“ ovom povredom nije zaprimio inicijalni neispravni izvod te je dokumentacija vraćena pošiljatelju, odnosno društvu Y. Nadalje, navodi se da će se nakon što se utvrdi da prethodno navedenih povrata više neće biti, na temelju dostavljenog provesti analiza kako bi se mogao ustanoviti broj klijenata koji su izuzeti od povrede, odnosno krajnji broj klijenata „pogođenih“ povredom bit će manji. Isto tako, društvo Y je o nastaloj povredi obavijestilo Hrvatsku narodnu banku kao i poslalo pisma isprike/obavijesti svim klijentima koji su u tom trenutku potencijalno zahvaćeni povredom.

Agencija je dopisom KLASA: __, URBROJ: __ od 8. svibnja 2024. od društva Y, zatražila očitovanje i dostavu popisa ispitanika kojima su dostavljeni neispravni izvodi i popis ispitanika koji nisu zaprimili neispravne izvode i isti su vraćeni Štedionici.

Dana 16. svibnja 2024. Agencija je zaprimila očitovanje i popratnu dokumentaciju od strane društva Y, kao voditelja obrade, u kojem je, između ostalog, dostavljen popis ispitanika kojima su dostavljeni neispravni izvodi s računa te ispitanika koji nisu zaprimili neispravne izvode jer su isti vraćeni društvu Y, a isti su kategorizirani po grupama: popis klijenata za koje je vraćena pošta koja je uključivala izvode računa trećih osoba, popis klijenata koji su bili predmet povrede, razvrstani po grupama prema kojima je slan dopis isprike i obavijesti o povredi te zbirna analitika svih klijenata prema broju ugovora i internom broju.

Također, dostavljen je popis po kategoriji i vrsti povrede koju zahvaćaju prema tri opisane kategorije iz nadopune Izvješća o povredi osobnih podataka od 21. veljače 2024. kako slijedi:

1. klijenti čiji su Izvodi s računa poslani drugim klijentima, no oni istovremeno nisu primili nijedan Izvod (niti svoj niti tuđi),
2. klijenti koji su uz Izvod koji glasi na njihovo ime zaprimili i Izvode s računa drugih klijenata (njihovi podaci nisu otkriveni trećim stranama),
3. klijenti čiji su Izvodi s računa poslani drugim klijentima, a istovremeno su i sami zaprimili tuđe.

U 1. kategoriju potpadaju ispitanici kojima su poslani dopisi broj 1 i broj 2, u 2. kategoriju potpadaju ispitanici kojima je slan dopis broj 3, dok su dopisi broj 4 i broj 5 slani 3. kategoriji ispitanika. Sukladno navodnom, ukupan broj ispitanika je 1649, a prema tipu povrede/vrsti dopisa razvrstani su kako slijedi: dopis broj 1 - 200 ispitanika, dopis broj 2 - 269 ispitanika, dopis broj 3 - 270 ispitanika, dopis broj 4 - 906 ispitanika i dopis broj 5 - 4 ispitanika.

Nadalje, navodi se da je za 5 klijenata koji su u nadopuni Izvješća o povredi bili uključeni u ukupan broj ispitanika (1654), utvrđeno je da do povrede nije došlo jer su njihovi izvodi bili prvi u datotekama za ispis te su bili samo nepotpuni, no njihove pošiljke nisu sadržavale nikakve tuđe niti neovlaštene podatke. Isto tako, navodi se da je u društvo Y vraćeno 26 pošiljki s krivo kuvertiranim izvodima računa unutar kojih su bili i podaci 28 osoba koji su poslani neovlaštenim primateljima.

Dana 22. kolovoza 2024. godine Agencija je provela nadzor kod izvršitelja obrade X, na adresi ___ na poslovnoj lokaciji gdje je smještaj radnih procesa i gdje je došlo do predmetne povrede istog izvršitelja obrade, te o tome sastavila zapisnik o provedenom nadzoru KLASA: __, URBROJ: __, kojim je utvrđeno da društvo X nema pisanu proceduru kontrole ispisa izvoda na strojevima ali da su, sukladno izjavama predstavnika izvršitelja obrade, cijeli sustav i procesi usklađeni sa standardom ISO 27001, da imaju više strojeva za poslove ispisa izvoda, da se provode edukacije zaposlenika za rad na strojevima, da se svaki put kada dođe novi stroj provodi edukacija od strane isporučitelja stroja te da se znanje o procesu obrade i kuvertiranju uglavnom usmeno prenosi s radnika na radnika.

Nadalje, predstavnik društva X je tijekom nadzora izjavio da nema posebne razlike između poslova koje zaprimaju od klijenata, da se radi o standardiziranim formama, da se vizualno razlikuju uglavnom po položaju bar koda i drugih detalja, a koje prilagođavaju po željama klijenata, da se u konkretnom slučaju radilo o izvodu koji se ispisuje jednom godišnje te da nije provedena ulazna kontrola zaprimljenog od društva Y.
Zapisniku je priložen *Obrazac obrade sigurnosnog događaja,* preslika dokumenta „*Osposobljavanje – evidencija prisutnih, Naziv osposobljavanja: Edukacija zaposlenika radi obnove znanja o pravilnom načinu upravljanja strojevima za kuvertiranje, podizanje svijesti o osjetljivosti procesa*“ od 23.02.2024, preslika „*Zapisnika o izvršenoj obuci operatera za rad na stroju za automatsko kuvertiranje Neopost DS-1200 i sustavom za verifikaciju slike na kuvertama“ s potpisima zaposlenika, od 02.10.2020.,* preslika *„Zapisnika o izvršenoj obuci operatera za rad na stroju za kuvertiranje Pitney Bowes Mailstream 26 na lokaciji tvrtke X*“ s potpisima zaposlenika, od 19.01.2024., preslika *„Protokola o razmjeni i kontroli datoteka za produkciju dokumenata“ od 22.03.2024.*

Dodatno je na zahtjev službenika Agencije predstavnik društva X, na svom računalu u uredu pored radne prostorije gdje se vrši ispis i kuvertiranje, opisao postupak zaprimanja zahtjeva za ispisom od strane klijenata, te prikazao korake i naveo da preuzima datoteku sa SFTP servera, da automatika podešena u informacijskom sustavu stvara tzv. „time stamp“, da se zaprimljena datoteka sprema pod imenom klijenta, da se provodi provjera zaprimljenog i nakon toga šalje u njihov sustav za postupak ispisa, zatim operater na stroju za printanje vidi u izlistanim radnim procesima koje treba provesti tzv. „spooler“ redom zadatke spremne za ispis i zatim pokreće zadatke po želji uzimajući u obzir moguće prioritete.

Također, tijekom nadzora ovlašteni službenici Agencije su proveli razgovor sa zaposlenicom __ na stroju koji je bio korišten za ispis izvoda društva Y u predmetnoj povredi, ali imenovana nije tada radila na istom stroju već druga zaposlenica koja je u trenutku nadzora bila na godišnjem odmoru, te je __ pokazala način zadavanja zadatka stroju, odabir postavki i modula koji je bio greškom odabran, a svezi postojanja kontrole odrađenih poslova ispisa na strojevima, predstavnik društva X je izjavio da postoje te da je to zaduženje zaposlenika čiji je opis radnog mjesta „operateri na printanju“ te da takva praksa postoji oduvijek.

Predstavnik društva X dodatno je tijekom nadzora priložio dokument *Izvještaj operatera o realizaciji po obavljenom zadatku* i pojasnio da se isti sastoji od rubrika „Zadatak na printanje“, „Podaci potrebni za kuvertiranje“ i „Podaci potrebni za distribuciju“ i operater na stroju po obavljenom poslu provjerava jesu li dobiveni rezultati identični onima navedenim na opisanom Izvještaju.

Nastavno na navedeno, ističemo kako se od 25. svibnja 2018., u svim državama članicama Europske unije, pa tako i u Republici Hrvatskoj, izravno i obvezujuće primjenjuje Opća uredba o zaštiti podataka.

Članak 2. Opće uredbe o zaštiti podataka propisuje kako se ista primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

Navedena Opća uredba o zaštiti podataka u članku 4. stavku 1. točki 1. propisuje da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Točkom 7. definirano je kako je voditelj obrade fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice. Točkom 8. definirano je kako je izvršitelj obrade fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

Sukladno članku 5. Opće uredbe o zaštiti podataka osobni podaci moraju biti zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika (načelo zakonitosti, poštenosti i transparentnosti); prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama (načelo ograničavanja svrhe); primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koju se obrađuju (načelo smanjenje količine podataka); točni i prema potrebi ažurni (načelo točnosti); čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju (načelo ograničenja pohrane); obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera (načelo cjelovitosti i povjerljivosti).

Nadalje, sukladno članku 6. Opće uredbe o zaštiti podataka obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega: (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; (d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe; (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka.

Člankom 28. stavkom 3. Opće uredbe o zaštiti podataka propisano je kako se obrada koju provodi izvršitelj obrade uređuje ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. U nastavku stavka taksativno su propisani obvezni sastojci takvog ugovora.

Isto tako, člankom 32. Opće uredbe o zaštiti podataka propisano je, između ostalog, kako 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, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade i (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, dok je stavkom 2. istoga članka propisano da se prilikom procjene odgovarajuće razine sigurnosti u obzir posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Provedenim uvidom u cjelokupnu dokumentaciju spisa predmeta, u ovoj upravnoj stvari utvrđeno je da je od strane društva X kao izvršitelja obrade zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka sukladno predvidivim rizicima, došlo do kršenja sigurnosti obrade koje je dovelo do neovlaštenog otkrivanja osobnih podataka ispitanika/klijenata društva Y neovlaštenim osobama na način da su dana 16. veljače 2024. ispisani i kuvertirani izvodi zbog greške u procesu obrade posljedično odaslani na primatelje na koje ne glase isti izvodi, a čime je zahvaćeno ukupno 1649 ispitanika.

Utvrđeno je da izvršitelj obrade X dana 15. veljače 2024. zaprimio datoteke od voditelja obrade, društva Y, putem kriptiranog kanala (SFTP), u pdf formatu, da je zahtjev za slanje pošiljaka na poštu bio 16. veljače 2024., da je u obradu datoteka krenuo 16. veljače 2024. ujutro, da je u tijeku procesa kuvertiranja posla „MFIN Krediti“ 16. veljače 2024. oko 12,00 sati došlo do kvara/zastoja na stroju za kuvertiranje, da kako bi ispunio zahtjev voditelja obrade za predaju pošiljki na poštu 16. veljače 2024., a čije vozilo dolazi u prikup pošiljki u 14,00 sati, odlučili su radnju kuvertiranja obaviti na drugom stroju za kuvertiranje.
Utvrđeno je da je na poštu predano 1205 komada kuverti, a količina je utvrđena na temelju „brojača“ na izlazu iz stroja za kuvertiranje, da je dana 20. veljače 2024., oko 15,00 sati dojavljeno od strane voditelja obrade kako im se javlja više komitenata koji su unutar kuverte primili svoj i tuđi izvod.

Utvrđeno je da je kod prebacivanja posla na drugi stroj za kuvertiranje i učitavanje konfiguracije postavki stroja, operater kuvertirki nepažnjom učitao pogrešni modul, što je rezultiralo pogrešnim čitanjem barkoda na dokumentima i pogrešnim grupiranjem, odnosno insertiranjem dokumenata u kuverte, na način da je zadnji list izvoda koji glasi na jednog ispitanika insertiran kao prvi list u novu kuvertu zajedno sa izvodima slijedećeg kredita, odnosno ugovora i tako nizom do kraja.

Utvrđeno je da je društvo Y provelo rekonstrukciju događaja te je na temelju iste utvrđeno da je riječ o 1204 kreditna predmeta koji su se na tiskarskom stroju ispisivali iz pet (5) „jobova“, no da se povreda odnosi na tarife za međufinanciranje kredita, a ne samo na K100 tarifu kako je inicijalno navedeno, da je ukupan broj ispitanika na koji se odnosi povreda 1649 budući da jedan kreditni predmet/Izvod u sebi može sadržavati informacije kako nositelja kredita, tako i članova obitelji koji su povezani s tim kreditom.

II. UTVRĐENJE UPRAVNE NOVČANE KAZNE

Člankom 44. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“ br. 42/18) je propisano da Agencija izriče upravne novčane kazne za povrede odredaba ovoga Zakona i Opće uredbe o zaštiti podataka, sukladno članku 83. Opće uredbe o zaštiti podataka.

Člankom 45. stavkom 1. navedenog Zakona je propisano da se upravne novčane kazne izriču odlukom. Temeljem stavka 2. istoga članka, odlukom će se utvrditi iznos i način uplate upravne novčane kazne. Odlukom se može utvrditi da se upravna novčana kazna plaća u obrocima. Temeljem stavka 4. istoga članka, protiv odluke nije dopuštena žalba, ali se može pokrenuti upravni spor pred nadležnim upravnim sudom.

Temeljem članka 46. istoga Zakona, upravna novčana kazna uplaćuje se u roku od 15 dana od dana pravomoćnosti odluke kojom je izrečena. Ako stranka u propisanom roku ne uplati upravnu novčanu kaznu odnosno po dospijeću zadnjeg obroka ako je odobreno obročno plaćanje, Agencija će obavijestiti Područni ured Porezne uprave Ministarstva financija na čijem je području prebivalište odnosno sjedište stranke kojoj je izrečena upravna novčana kazna, radi naplate upravne novčane kazne prisilnim putem prema propisima o prisilnoj naplati poreza. Upravne novčane kazne uplaćuju se u korist državnog proračuna. Iznimno od stavka 2. ovoga članka, na dospjelu, a neplaćenu upravnu novčanu kaznu ne obračunava se kamata.

S obzirom na utvrđene okolnosti u konkretnom slučaju Agencija je sukladno svojim ovlastima iz članka 58. stavka 2. točke (i) Opće uredbe o zaštiti podataka izrekla upravnu novčanu kaznu umjesto drugih korektivnih mjera iz predmetnog članka, a sve u skladu s uvjetima za njezino izricanje iz članka 83. Opće uredbe o zaštiti podataka i članka 44., 45. i 46. Zakona o provedbi Opće uredbe o zaštiti podataka. Nakon detaljnog razmatranja raspoloživih korektivnih mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka, a koje nadzorno tijelo ima ovlasti izreći voditelju obrade, u slučaju kršenja odredbi Opće uredbe o zaštiti podataka, te cijeneći sve okolnosti predmetnog slučaja, a posebno da odabrana korektivna mjera mora biti učinkovita, proporcionalna i odvraćajuća u svakom pojedinom slučaju, Agencija je odlučila izreći upravnu novčanu kaznu posvećujući dužnu pozornost kriterijima propisanim člankom 83. stavkom 2. Opće uredbe o zaštiti podataka.

Naime, člankom 83. stavkom 1. Opće uredbe o zaštiti podataka propisano je da svako nadzorno tijelo osigurava da je izricanje upravnih novčanih kazni u skladu s ovim člankom u pogledu kršenja Opće uredbe o zaštiti podataka iz stavaka 4., 5. i 6. u svakom pojedinačnom slučaju učinkovito, proporcionalno i odvraćajuće.

Agencija smatra da iznos izrečene upravne novčane kazne ne može biti učinkovit ako nema značajan utjecaj na prihode izvršitelja obrade, načelo proporcionalnosti ne može se održati ako se povreda razmatra apstraktno bez obzira na utjecaj na voditelja ili izvršitelja obrade, a ista treba biti i odvraćajuća od budućih kršenja. Dakle, izrečena upravna novčana kazna ne može biti odvraćajuća ako nema financijskog utjecaja na voditelja/izvršitelja obrade.
Izricanjem upravne novčane kazne ujedno se želi postići da se poštuju pravila o zaštiti osobnih podataka kako od strane samog voditelja obrade tako i od svih drugih voditelja/izvršitelja obrade koji obrađuju osobne podatke ispitanika. Izricanjem upravne novčane kazne treba se postići generalno odvraćanje (obeshrabriti druge u ponavljanju istog kršenja u budućnosti), kao i posebno odvraćanje (obeshrabriti adresata ove upravne novčane kazne od ponavljanja istog kršenja).

Temeljem članka 83. stavka 2. Opće uredbe o zaštiti podataka, upravne novčane kazne izriču se uz mjere ili umjesto mjera iz članka 58. stavka 2. točaka od (a) do (h) i članka 58. stavka 2. točke (j), ovisno o okolnostima svakog pojedinog slučaja. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna se pozornost posvećuje sljedećem:

(a) prirodi, težini i trajanju kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli;
(b) ima li kršenje obilježje namjere ili nepažnje;
(c) svakoj radnji koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici;
(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32.;
(e) svim relevantnim prijašnjim kršenjima voditelja obrade ili izvršitelja obrade;
(f) stupnju suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja;
(g) kategorijama osobnih podataka na koje kršenje utječe;
(h) načinu na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju;
(i) ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera;
(j) poštovanju odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42.; i
(k) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

Sukladno članku 83. stavku 3. Opće uredbe o zaštiti podataka ako voditelj obrade ili izvršitelj obrade za istu ili povezane obrade namjerno ili iz nepažnje prekrši nekoliko odredaba ove Uredbe ukupan iznos novčane kazne ne smije biti veći od administrativnog iznosa utvrđenog za najteže kršenje.

U članku 83. stavku 4. Opće uredbe o zaštiti podataka propisano je kako se za obveze voditelja i izvršitelja obrade iz članka 25. do 39. mogu izreći upravno novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće.

Budući da ukupni godišnji promet na svjetskoj razini u 2023. godini za X iznosi 7.734.180,47 EUR, 2% tog iznosa je 154.683,60 EUR, što je manje od 10.000.000,00 EUR, odnosno iznosa koji predstavlja gornju granicu za izricanje upravne novčane kazne u konkretnom slučaju.

Agencija je radi kršenja članka 32. Opće uredbe o zaštiti podataka izrekla društvu X upravnu novčanu kaznu u iznosu od 17.500,00 Eura, a koji iznos čini 0,175% u odnosu na maksimalni iznos upravne novčane kazne koju je u konkretnom slučaju Agencija mogla, odnosno bila ovlaštena izreći.

Na temelju odredbe članka 83. stavka 2. Opće uredbe o zaštiti podataka, pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne, Agencija je u ovom slučaju dužnu pozornost posvetila sljedećem:

- Priroda, težina i trajanje kršenja, uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli (članak 83. stavak 2, točka a);

U predmetnom slučaju, kako je utvrđeno u točki 1. izreke ovog rješenja, došlo je do kršenja obveza iz članka 32. Opće uredbe o zaštiti podataka, neprovođenjem odgovarajućih tehničkih i organizacijskih mjera sigurnosti obrade osobnih podataka od strane izvršitelja obrade X, a za koje kršenje Opća uredba o zaštiti podataka propisuje izricanje upravne novčane kazne sukladno članku 83. stavku 4. točke a), odnosno, upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno što je veće.

Sukladno Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679, pokazatelj težine kršenja može biti ne samo priroda kršenja, već i opseg, svrha predmetne obrade kao i broj ispitanika i razina štete koju su pretrpjeli.

U predmetnoj povredi je utvrđeno da je istom zahvaćeno 1649 ispitanika zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera zaštite obrade u procesu ispisa Izvoda koji su sadržavali osobne podatke ispitanike voditelja obrade Y.
Iako predmetna povreda može biti sagledana u vremenskom okviru kad se dogodila, odnosno, na dan 16. veljače 2024., kršenje odredbi Opće uredbe o zaštiti podataka izvršitelja obrade zapravo traje od 15.01.2019. od početka trajanja ugovornog odnosa s voditeljem obrade Y temeljem Ugovora o okvirima poslovne suradnje __ od 15.01.2019., Sporazuma o zaštiti osobnih podataka br. __ od 15.01.2019. i Ugovora o produkciji dokumenata od 15.01.2019., jer izvršitelj obrade X nije implementirao odgovarajuće mjere sigurnosti koje su mogle, odnosne trebale svesti rizik iste ili slične povrede na najmanju moguću razinu.

- Ima li kršenje obilježje namjere ili nepažnje (članak 83. stavak 2, točka b);

Radna skupina iz članka 29 navodi u Smjernicama o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 da “namjera” u pravilu uključuje znanje i nakanu u pogledu značajki prekršaja, dok “nenamjerno” znači da nije postojala namjera da se prouzroči kršenje iako je voditelj obrade/izvršitelj obrade prekršio svoju obvezu dužne pažnje propisanu zakonom. Iste Smjernice dakle naglašavaju razliku između okolnosti koje su indikativne ili „namjerne povrede“ i onih koje ukazuju na kršenja koja su prouzročena „nenamjerno“ ili “nemarom“. U tom smislu Smjernice navode "ne donošenje politika" i "ljudsku pogrešku" kao primjere ponašanja koji mogu ukazivati na nepažnju.

U odnosu na navedeno, u predmetnom slučaju nije utvrđeno da je bilo izravne namjere kršenja odredbi Opće uredbe o zaštiti podataka od strane X, ali je utvrđen nemar i nedostatak radnji koje bi prevenirale povredu.
Naime, u ovoj upravnoj stvari utvrđeno je da je X, kao izvršitelj obrade propustio primijeniti odgovarajuće organizacijske i tehničke mjere zaštite kako bi zaštitio osobne podatke koje obrađuje, odnosno zaštitio osobne podatke od zabranjenog odavanja i neovlaštenog pristupa, što je imalo za posljedicu, kada je ispis Izvoda nakon kvara na prvom stroju na kojem je započet

dovršen na drugom stroju, da su isti Izvodi odaslani osobama na koje ne glase, a da pri tome nisu prethodno provjereni svi parametri potrebni za dobivanje točnih rezultata, niti su bili implementirani sigurnosni mehanizmi za otkrivanje greške, čime su ispunjeni svi elementi grube nepažnje u postupanju.

- Svaka radnja koju je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici (članak 83. stavak 2., točka c);

Nastavno na saznanje o predmetnoj povredi X je aktivno surađivao s voditeljem obrade na utvrđenju svih okolnosti iste povrede što je između ostalog rezultiralo da je voditelj obrade Y nakon točne identifikacije klijenata prema prethodno definiranoj vrsti povrede pripremio službene obavijesti kako bi svakog pojedinog klijenta izravno obavijestio o povredi i situaciji primjenjivoj na njega te dao uputu za daljnje postupanje.

- Stupanj odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32. (članak 83. stavak 2 točka d);

Uzimajući u obzir odredbe članka 32. koje obvezuju voditelja obrade i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade; proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade, da se prilikom procjene odgovarajućeg nivoa sigurnosti posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka, ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, utvrđeno je da X provodi određene organizacijske i tehničke mjere zaštite pri obradi osobnih podataka, ali da u konkretnom slučaju nisu bile dovoljne, čime je došlo do neovlaštenog otkrivanja osobnih podataka ispitanika.

Utvrđeno je da izvršitelj obrade X u trenutku predmetne povrede nije imao usvojene interne akte kojima se propisuje procedura zaprimanja zadataka na ispis od strane klijenata, koraci u procesu ispisa izvoda, uloge i zadaci zaposlenika te potrebne akcije za osiguranje točnosti ispisa.

Utvrđeno je da izvršitelj obrade X u trenutku predmetne povrede nije imao usvojen interni akt kojim se propisuje postupanje u slučaju kvara ili zastoja rada na stroju na kojem je započet proces ispisa te prelazak na zamjenski stroj koji treba dovršiti proces ispisa ili započeti isti proces ispočetka te provedba kontrole dobivenih rezultata ispisa prije otpreme voditelju obrade.

Utvrđeno je da izvršitelj obrade X u trenutku predmetne povrede nije imao usvojene interne akte odnosne na obuku zaposlenika za rad na pojedinom stroju koji se koristi u procesu ispisa Izvoda, već se znanje o procesu obrade i kuvertiranju uglavnom usmeno prenosi s radnika na

radnika, odnosno, edukacija zaposlenika za rad na novom stroju se provodi od strane isporučitelja stroja ali to ne rezultira stvaranjem trajnog dokumenta/uputa za rad na stroju koji će uključivati i dio odnosan na sigurnost obrade osobnih podataka.

Utvrđeno je da izvršitelj obrade X u trenutku predmetne povrede nije imao implementirano tehničko rješenje/kontrolni mehanizam koje će pravovremeno detektirati grešku u procesu ispisa dokumenata i izvijestiti nadležne osobe na moguću povredu osobnih podataka.

- Relevantna prijašnja kršenja voditelja obrade ili izvršitelja obrade (članak 83. stavak 2. točka e);

Prema evidencijama kršenja koje vodi ova Agencija, društvo X nije u prošlosti počinilo istovjetno kršenje niti je prekršilo Opću uredbu o zaštiti podataka na istovjetan način.

- Stupanj suradnje s nadzornim tijelom kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja (članak 83. stavak 2. točka f);

Društvo X je tijekom ovog upravnog postupka na odgovarajući način odgovaralo na zahtjeve nadzornog tijela.

- Kategorije osobnih podataka na koje kršenje utječe (članak 83. stavak 2. točka g);

Tijekom postupka je utvrđeno da je predmetnom povredom obuhvaćena osnovna kategorija osobnih podataka i to svi podaci koji su sadržani na Izvodu s računa klijenta voditelja obrade Y (ime, prezime, adresa, broj ugovora o kreditu/štednji vezanoj uz kredit, podaci o prometu po računu).

- Način na koji je nadzorno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri voditelj obrade ili izvršitelj obrade izvijestio o kršenju (članak 83. stavak 2. točka h);

Za predmetnu povredu kod izvršitelja obrade X nadzorno tijelo je saznalo od voditelja obrade Y putem zaprimljenog Izvješća o povredi osobnih podataka od 21. veljače 2024., a koje je isti poslao nakon što je tijekom 19. i 20. veljače 2024. u nekoliko navrata i telefonskim putem i e-mailom zaprimio prijave klijenata koji su na svojoj kućnoj adresi zaprimili neispravne Izvode s računa, odnosno Izvode s računa koji djelomično sadrže podatke s Izvoda i drugih klijenata Štedionice, a ne samo ciljanih primatelja.

- Ako su protiv dotičnog voditelja obrade ili izvršitelja obrade u vezi s istim predmetom prethodno izrečene mjere iz članka 58. stavka 2., poštovanju tih mjera (članak 83. stavak 2. točka i);

Društvu X u vezi s istim predmetom nije prethodno izrečena mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka.

- Poštovanje odobrenih kodeksa ponašanja u skladu s člankom 40. ili odobrenih mehanizama certificiranja u skladu s člankom 42. (članak 83. stavak 2. točka j);
Nije primjenjivo u predmetnom slučaju.

- Svi ostali otegotni ili olakotni čimbenici koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem (članak 83. stavak 2. točka k);

Nije utvrđeno da je X ostvario financijsku dobit kršenjem niti izbjegnuo gubitke, izravno ili neizravno. Međutim, Agencija otegotnom okolnošću nalazi u činjenici da je osnovna djelatnost društva X ispisivanje i kuvertiranje dokumenata zaprimljenih od više voditelja obrade, da u svakodnevnom radu u svojim radnim procesima obrađuju veliki broj osobnih podataka ispitanika, da je s obzirom na predvidive rizike bilo za očekivati da će predmetno društvo implementirati složenije organizacijske i tehničke mjere koje će povredu istu ili sličnu predmetnoj prevenirati ili svesti na najmanju moguću mjeru.

Slijedom svega navedenog, a temeljem odredbe članka 42. i 96. Zakona o općem upravnom postupku („Narodne novine“ br. 47/09 i 110/21), odlučeno je kao u izreci Rješenja.

UPUTA O PRAVNOM LIJEKU

Protiv ovog rješenja žalba nije dopuštena, ali se može pokrenuti upravni spor pred Upravnim sudom u __ u roku od 30 dana od dana dostave rješenja.

DOSTAVITI:
1. X,
2. Pismohrana, ovdje