HRVATSKA AGENCIJA ZA MALO GOSPODARSTVO, INOVACIJE I INVESTICIJE

PROCEDURA
O POSTUPANJU U SLUČAJU POVREDE OSOBNIH PODATAKA

Zagreb, veljača 2025. godine

SADRŽAJ

Na temelju odredbi članaka 24., 25. i 32., 33. i 34. 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) te odredbe članka 17. Statuta Hrvatske agencije za malo gospodarstvo, inovacije i investicije (Narodne novine, br. 107/14, 72/15, 116/15, 97/17, 29/21), Uprava dana 3. veljače 2025. godine

donosi sljedeću:

P R O C E D U R U

o postupanju u slučaju povrede osobnih podataka

I. ZNAČENJE POJMOVA

U odnosu na potrebe ove Procedure o postupanju u slučaju povrede osobnih podataka , niže navedeni pojmovi imaju ovdje ima dana značenja kako slijedi.

- ***Procedura*** znači ova Procedura o postupanju u slučaju povrede osobnih podataka;
- ***Opća uredba*** znači UREDBU (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*);
- ***Zakon o provedbi Opće uredbe*** znači Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine 42/2018) kojim je provedena Opća uredba u nacionalno zakonodavstvo;
- ***Obrada*** znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;
- ***osobni podatak / podatci*** znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (ispitanik);
- ***Agencija*** znači Hrvatska agencija za malo gospodarstvo, inovacije i investicije sa sjedištem na adresi Ksaver 208, 10000 Zagreb, OIB 25609559342;
- ***radnici*** znači svakog pojedinca - radnika koji je u odnosu s Agencijom temeljem ugovora o radu, pojedinca - studenta koji je u odnosu s Agencijom temeljem ugovora o obavljanju studentskog posla;

- ***ispitanik*** znači pojedinac čiji je identitet utvrđen ili se može utvrditi; 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;

- ***voditelj obrade*** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka;

- ***izvršitelj obrade*** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;

- ***zajednički voditelj obrade*** znači dvoje ili više voditelja obrade koji zajednički odrede svrhe i načine obrade osobnih podataka;

- ***primatelj*** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;

- ***treća strana*** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;

- ***nadzorno tijelo*** znači neovisno tijelo javne vlasti koje je osnovala država članica; u Republici Hrvatskoj to je Agencija za zaštitu osobnih podataka (AZOP), Ulica grada Vukovara 54, 10000 Zagreb, Hrvatska;

- ***službenik*** znači službenik za zaštitu podataka;

- ***odgovorna osoba*** znači ravnatelj ili osoba koju ovlasti ravnatelj;

- ***Europska unija*** znači međuvladina i nadnacionalna organizacija 27 europskih država kojoj su ciljevi gospodarska i politička integracija europskoga kontinenta;

- ***međunarodna organizacija*** znači organizacija i njezina podređena tijela uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na osnovi sporazuma osnovale dvije ili više zemalja;

- ***sigurnosni incident*** znači svaki štetni događaj koji ugrožava različite aspekte sigurnosti, a posebno povjerljivost, cjelovitost i raspoloživost podataka; svaki sigurnosni incident nužno ne znači i povredu osobnih podataka, no svaka povreda osobnih podataka predstavlja sigurnosni incident;

- ***povreda osobnih podataka*** znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

II. PREDMET I SVRHA PROCEDURE

Ova Procedura predstavlja jednu od organizacijskih mjera predviđenih Općom uredbom i najboljom važećom praksom u području zaštite osobnih podataka i privatnosti, a koju je Agencija implementirala u svoje poslovanje u svrhu usklađenja poslovanja sa zahtjevima Opće uredbe.

Ova Procedura, kao organizacijska mjera, donesena je u svrhu osiguranja odgovarajuće sigurnosti osobnih podataka.

Ovom se Procedurom uređuje postupanje u slučaju sumnje na povredu ili nastanka povrede osobnih podataka.

Ova Procedura primjenjuje se na Agenciju te njene radnike kada dolaze u doticaj, odnosno kada obrađuju osobne podatke ispitanika. U svrhu izbjegavanja svake sumnje, prava i obveze navedeni u ovoj Proceduri, na jednak način odnose se i na osobe koje Agencija angažira temeljem ugovora o djelu ili druge pravne osnove u slučajevima u kojima obavljaju poslove kao radnici.

Agencija će upoznati, odnosno educirati sve radnike o pravima i obvezama koji proizlaze iz ove Procedure.

III. PROVEDBA NAČELA SIGURNOSTI OBRADE OSOBNIH PODATAKA

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, Agencija provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurala odgovarajuću razinu sigurnosti za osobne podatke koje obrađuje.

Agencija u odnosu na sigurnost osobnih podataka te sigurnost sustava i načina obrade istih, primjenjuje načela povjerljivosti, cjelovitosti, dostupnosti i otpornosti, na način opisan u niže navedenim odredbama.

Načelo povjerljivosti Agencija primjenjuje na način da osobnim podatcima mogu pristupiti, izmijeniti ih, otkriti ili izbrisati samo ovlašteni pojedinci u okviru ovlasti i uputa koje su im dane.

Načelo cjelovitosti Agencija primjenjuje na način da su osobni podatci koji se obrađuju točni i potpuni u odnosu na svrhu obrade.

Načelo dostupnosti Agencija primjenjuje na način da su osobni podatci uvijek dostupni i upotrebljivi, odnosno da se osobni podatci mogu povratiti u razumnom roku ako dođe do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa.

Načelo otpornosti Agencija primjenjuje na način da u slučaju nepovoljnih sigurnosnih uvjeta se osigurava daljnji rad sustava obrade osobnih podataka, kao i učinkovito vraćanje istih u potpuno funkcionalno stanje. Također, primjenjuje se i kroz redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguranje sigurnosti obrade.

IV. POVREDA OSOBNIH PODATAKA

Povreda osobnih podataka predstavlja vrstu sigurnosnog incidenta. Ako sigurnosni incident ne uključuje osobne podatke, ne smatra se povredom osobnih podataka.

Do povrede osobnih podataka može doći zbog fizičkog ili tehničkog incidenta te se odnosi samo na osobne podatke koji su se obrađivali prije same povrede, dakle ne odnosi se na osobne podatke koji će se obrađivati ubuduće.

Povredom osobnih podataka smatra se svaka povreda, slučajna i namjerna.

Ovisno o riziku od nastanka posljedica povrede osobnih podataka, odnosno negativnih učinaka na ispitanike, Agencija će odlučiti o daljnjem postupanju u odnosu na nastalu povredu.

V. OPĆENITO O OBVEZAMA U ODNOSU NA POVREDE OSOBNIH PODATAKA

Radnici su dužni poštivati interna pravila Agencije koja se odnose na zaštitu osobnih podataka i privatnost. Više o pravima i obvezama radnika u odnosu na zaštitu osobnih podataka i privatnost nalazi se u *Pravilniku o postupanju s osobnim podatcima* te ostaloj dokumentaciji koju je Agencija donijela u svrhu zaštite osobnih podataka.

U slučaju da nastala povreda obuhvaća i druge vrste sigurnosnih incidenata koji su regulirani drugim internim propisima Agencije, radnik je dužan postupati kako temeljem odredbi ove Procedure, tako i temeljem odredbi drugih internih propisa koji se tiču nastalog sigurnosnog incidenta.

U svrhu izbjegavanja svake sumnje, radnici su educirani da mogu prepoznati povredu osobnih podataka.

VI. POSTUPANJE U SLUČAJU SAZNANJA I / ILI OTKRIVANJA POVREDE

U slučaju kada radnik sazna za i / ili otkrije povredu osobnih podataka, dužan je bez odgađanja o istoj obavijestiti službenika. U slučaju sumnje na povredu osobnih podataka, radnik je dužan postupiti na jednak način kao da je saznao za i / ili otkrio povredu osobnih podataka.

U slučaju kada radnik sazna za i / ili otkrije sigurnosni incident za koji ne može procijeniti s potpunom sigurnošću obuhvaća li i povredu osobnih podataka, dužan je postupiti na jednak način kao da je saznao za i / ili otkrio povredu osobnih podataka.

U slučaju kada radnik sazna za i / ili otkrije ili sumnja na povredu osobnih podataka, dužan je učinit sve što može kako bi zaustavio i / ili spriječio daljnju neovlaštenu obradu.

U slučaju kada Agencija, odnosno netko od radnika Agencije, bude obaviješten o povredi osobnih podataka od strane nekoga izvan Agencije (*na primjer od ispitanika, iz medija i slično*), dužan je bez odgađanja o saznanju obavijestiti službenika. U slučaju sumnje radi li se o povredi osobnih podataka ili ne, radnik koji je bio obaviješten dužan je bez odgađanja o saznanju obavijestiti službenika.

U slučaju kada Agencija, odnosno netko od radnika Agencije, bude obaviješten o sigurnosnom incidentu za koji ne može procijeniti s potpunom sigurnošću obuhvaća li i povredu osobnih podataka, dužan je bez odgađanja o saznanju obavijestiti službenika.

VII. PRELIMINARNA ISTRAGA I UTVRĐIVANJE POVREDE

Službenik, uz pomoć radnika koji je saznao za i / ili otkrio ili bio obaviješten o povredi osobnih podataka, dužan je provesti preliminarnu istragu radi utvrđivanja je li zaista došlo do povrede osobnih podataka. Predmetna istraga mora se provesti u roku ne dužem od 24 (*dvadeset i četiri*) sata od saznanja ili obavještavanja radnika o povredi osobnih podataka.

U slučaju kada je Agencija bila obaviještena o povredi osobnih podataka od strane nekoga izvan Agencije, u slučaju potrebe, moguće je od osobe izvan Agencije zatražiti dodatne informacije.

Preliminarna istraga se provodi na način da se nastala povreda dokumentira, odnosno da se sastavi detaljan zapisnik o povredi te prikupe svi relevantni dokazi i dokumentacija. Obrazac zapisnika o povredi osobnih podataka čini *Prilog broj 1 ovoj Proceduri*.

Temeljem provedene preliminarne istrage, službenik utvrđuje je li došlo do povrede osobnih podataka ili ne.

Službenik je dužan zapisnik o povredi osobnih podataka zajedno sa svim relevantnim dokazima i dokumentacijom, bez odgađanja i u najkraćem mogućem roku, dostaviti odgovornoj osobi Agencije na znanje. Također, dužan je uputit odgovornu osobu Agencije u rezultate preliminarne istrage.

Ako preliminarnom istragom nije utvrđena povreda osobnih podataka, isto je dužna potvrditi odgovorna osoba Agencije.

Ako je preliminarnom istragom utvrđena povreda osobnih podataka te se odgovorna osoba Agencije slaže s predmetnim nalazom, službenik zajedno s odgovornom osobom pristupa procjeni rizika nastale povrede i donošenju odluke o daljnjem postupanju.

U slučaju neslaganja odgovorne osobe Agencije sa zaključkom preliminarne istrage, odgovorna osoba donosi konačnu odluku o daljnjem postupanju.

Procjena rizika i odluka o daljnjem postupanju mora se provesti / donijeti bez odgode, a najkasnije u roku od 48 (*četrdeset i osam*) sati od saznanja radnika za povredu.

VIII. PROCJENA RIZIKA

Na temelju informacija iz zapisnika o povredi osobnih podataka, relevantnih dokaza i dokumentacije službenik će zajedno s odgovornom osobom Agencije izvršit procjenu rizika nastale povrede na osobne podatke ispitanika.

Rizik se procjenjuje temeljem objektivne procjene, posebno uzimajući u obzir vjerojatnost i ozbiljnost rizika za prava i slobode ispitanika.

Pri procjeni rizika, osim informacija iz zapisnika o povredi osobnih podataka te relevantnih dokaza i dokumentacije, potrebno je uzeti u obzir sljedeće kriterije:

- *vrstu povrede osobnih podataka,*
- *prirodu, osjetljivost i količinu osobnih podataka obuhvaćenih povredom,*
- *lakoću identificiranja ispitanika iz osobnih podataka obuhvaćenih povredom,*
- *ozbiljnost posljedica povrede osobnih podataka na ispitanike,*
- *posebna obilježja ispitanika čiji su osobni podatci obuhvaćeni povredom,*
- *posebna obilježja Agencije u odnosu na vezu s ispitanicima čiji su osobni podatci obuhvaćeni povredom,*
- *broj ispitanika čiji su osobni podatci obuhvaćeni povredom,*
- *druge važne kriterije.*

Rezultati procjene rizika dokumentiraju se u zapisniku koji čini *Prilog broj 1 ovoj Proceduri.*

IX. ODLUKA O DALJNJEM POSTUPANJU

Ako službenik zajedno s odgovornom osobom Agencije ocjeni kako je nastala povreda prouzročila ili će prouzročiti rizik za prava i slobode ispitanika, Agencija je dužna donijeti službenu odluku o obavještavanju nadzornog tijela o nastaloj povredi u skladu s pravilima o obavještavanju nadzornog tijela.

Ako službenik zajedno s odgovornom osobom Agencije ocjeni kako je nastala povreda prouzročila ili će prouzročiti visok rizik za prava i slobode ispitanika, odnosno fizičku, materijalnu ili nematerijalnu štetu za ispitanike, Agencija je dužna donijeti službenu odluku o obavještavanju ispitanika o nastaloj povredi u skladu s pravilima o obavještavanju ispitanika.

Ako službenik zajedno s odgovornom osobom Agencije ocjeni kako nastala povreda ne stvara rizik za prava i slobode ispitanika, Agencija je dužna donijeti službenu odluku kako neće obavijestiti nadzorno tijelo i ispitanike o nastaloj povredi. Predmetnu odluku dužni su posebno obrazložiti te dokumentirati zajedno sa zapisnikom o povredi osobnih podataka, relevantnim dokazima i ostalom dokumentacijom.

U slučaju dvojbe treba li obavijestiti nadzorno tijelo o nastaloj povredi osobnih podataka, Agencija će donijeti službenu odluku o obavještavanju nadzornog tijela o nastaloj povredi u skladu s pravilima navedenim u ovoj Proceduri.

U slučaju dvojbe treba li obavijestiti ispitanike o nastaloj povredi osobnih podataka, Agencija će kontaktirati i savjetovati se s nadzornim tijelom te postupiti po uputi nadzornog tijela.

Agencija zadržava pravo da ne obavijesti ispitanika o nastaloj povredi osobnih podataka u sljedećim slučajevima:

- *ako su poduzete odgovarajuće tehničke i organizacijske mjere zaštite nad osobnim podatcima koji su predmetom povrede,*

- *ako su poduzete naknadne mjere koje osiguravaju da neće doći do visokog rizika za prava i slobode ispitanika čiji su osobni podatci obuhvaćeni povredom.*

X. OBAVJEŠTAVANJE NADZORNOG TIJELA

Temeljem odluke Agencije o obavještavanju nadzornog tijela o nastaloj povredi osobnih podataka, službenik će obavijestit nadzorno tijelo o nastaloj povredi na propisanom obrascu koje je objavilo nadzorno tijelo na svojim mrežnim stranicama. Predmetni obrazac čini sastavni dio dokumentacije Agencije koja se odnosi na zaštitu osobnih podataka i privatnost. Popunjenom obrascu nadzornog tijela prilažu se popunjeni zapisnik o povredi osobnih podataka koji čini *Prilog broj 1 ovoj Proceduri* te ostali relevantni dokazi i dokumentacija.

Agencija će obavijestiti nadzorno tijelo bez odgađanja, odnosno najkasnije u roku od 72 (*sedamdeset – dva*) sata od saznanja radnika za nastalu povredu.

U situacijama u kojima nije moguće nadzornom tijelu dostaviti sve informacije o nastaloj povredi osobnih podataka u rok od 72 (*sedamdeset-dva*) sata od saznanja radnika za nastalu povredu, odnosno potrebno je provesti daljnju (naknadnu) istragu i praćenje, Agencija će obavijestiti nadzorno tijelo kako će, osim dostavljenih informacija i dokumentacije, postupno i bez nepotrebnog odgađanja dostavljati i druge informacije u vezi nastale povrede osobnih podataka.

Agencija će se s nadzornim tijelom dogovoriti oko načina i vremena dostavljanja dodatnih informacija. Ako Agencija sazna dodatne relevantne pojedinosti o povredi, može ih dostaviti nadzornom tijelu u bilo kojem trenutku, neovisno o dogovoru u vezi načina i vremena dostave dodatnih informacija.

U slučaju kada daljnja istraga Agencije pokaže kako je povreda osobnih podataka bila spriječena na vrijeme i nije proizvela rizik za prava i slobode ispitanika, odnosno da se nije dogodila povreda osobnih podataka, Agencija će nadzornom tijelu dostaviti ažurirane informacije te zatražiti evidentiranje novih okolnosti, odnosno okolnosti kako nije došlo do povrede osobnih podataka u nastalom sigurnosnom incidentu.

U slučaju kada Agencija propusti izvijestiti nadzorno tijelo o nastaloj povredi osobnih podataka u rok od 72 (*sedamdeset-dva*) sata od saznanja radnika za nastalu povredu, Agencija će prilikom obavještavanja nadzornog tijela dostaviti obrazloženje razloga kašnjenja.

U slučaju nastanka niza jednakih i / ili vrlo sličnih povreda istih kategorija osobnih podataka u vrlo kratkom razdoblju, Agencija može obavijestiti nadzorno tijelo o predmetnim povredama putem jedne, objedinjene obavijesti.

U slučaju nastanka niza različitih povreda različitih kategorija osobnih podataka u vrlo kratkom razdoblju, Agencija je dužna obavijestiti nadzorno tijelo na uobičajen način, odnosno pojedinačno o svakoj povredi osobnih podataka.

XI. OBAVJEŠTAVANJE ISPITANIKA

Temeljem odluke Agencije o obavještavanju ispitanika o nastaloj povredi osobnih podataka, službenik će obavijestit ispitanike o nastaloj povredi osobnih podataka putem obrasca koji čini *Prilog broj 2 ovoj Proceduri*. Predmetni obrazac čini sastavni dio dokumentacije Agencije koja se odnosi na zaštitu osobnih podataka i privatnost.

Agencija će obavijestiti ispitanika o nastaloj povredi bez odgađanja, istovremeno s obavještavanjem nadzornog tijela, osim u slučaju sumnje za potrebom obavještavanja ispitanika kada je dužna postupiti u skladu s pravilima koja se odnose na donošenje odluke o daljnjem postupanju.

Ako se radi o manjem broju ispitanika obuhvaćenih nastalom povredom te Agencija raspolaže s dovoljno njihovih osobnih podataka da stupi s njima u kontakt, Agencija će predmetne ispitanike pojedinačno i izravno obavijestiti o nastaloj povredi putem uobičajenih kanala komunikacije (na primjer slanjem obavijesti na adrese elektroničke pošte, slanjem preporučenog pismena s povratnicom na odgovarajuću adresu ispitanika i slično).

Ako se radi o većem broju ispitanika i / ili se ne može utvrditi koji sve ispitanici su obuhvaćeni nastalom povredom osobnih podataka, dakle bilo bi nerazmjerno teško obavijestiti ispitanike pojedinačno, Agencija će ih obavijestiti javno putem svoje internetske stranice.

Ako se radi o manjem broju ispitanika obuhvaćenih nastalom povredom, no Agencija ne raspolaže s potpunim osobnim podatcima nekih ispitanika te iste ne može obavijestiti pojedinačno i izravno o nastaloj povredi osobnih podataka, Agencija će uz izravno obavještavanje onih ispitanika čijim osobnim podatcima raspolaže, obavijestiti ispitanike i javno putem svoje internetske stranice. Osim navedenog, svakom takvom ispitaniku koji nije bio obavješten pojedinačno i izravno, bit će poslana obavijest o nastaloj povredi čim je to razumno izvedivo (na primjer prilikom prvog kontakta s ispitanikom).

U slučaju kada Agencija provođenjem naknadne istrage otkrije druge relevantne činjenice koje imaju važan utjecaj na rizik za prava i slobode ispitanika, Agencija će ispitanike dodatno obavijestiti o predmetnim činjenicama u skladu s pravilima o obavještavanju ispitanika.

XII. MJERE ZA SPRJEČAVANJE DALJNJIH POVREDA

Osim obveze radnika koji sazna za i / ili otkrije ili sumnja na povredu osobnih podataka u skladu s pravilima o postupanju u slučaju saznanja i / ili otkrivanja povrede osobnih podataka, odmah po utvrđivanju službenika kako je došlo do povrede osobnih podataka te po obavještavanju odgovorne osobe Agencije o istoj, Agencija je dužna bez odgađanja poduzeti sve tehničke i organizacijske mjere kako bi spriječila nastanak daljnjih povreda, umanjila rizik i posljedice nastale povrede te ponovno uspostavila sigurnu obradu osobnih podataka.

Sve poduzete tehničke i organizacijske mjere (*npr. mjere poput zabrane pristupa računalima / programskim rješenjima, donošenje odluke / procedure o ograničenom pravu pristupa, imenovanje osobe za saniranje štete nastale od povrede, izrade sigurnosnih kopija, analiza povrede i slično*) Agencija je dužna dokumentirati u zapisniku koji čini *Prilog broj 1 ovoj Proceduri.*

Ako je potrebno provoditi naknadnu istragu o nastaloj povredi osobnih podataka nakon preliminarne, ovisno o nalazima naknadne istrage, potrebno je prilagođavati i nastaviti s primjenom tehničkih i organizacijskih mjera. Predmetne tehničke i organizacijske mjere potrebno je dokumentirati u skladu s pravilima o provođenju mjera za sprječavanje daljnjih povreda i umanjivanja posljedica nastale povrede.

XIII. NAKNADNA ISTRAGA

Kada preliminarnom istragom nije bilo moguće obuhvatiti sve relevantne činjenice nastale povrede osobnih podataka, Agencija je dužna provesti naknadnu istragu. Nalaze naknade istrage potrebno je dokumentirati te unijeti u postojeći zapisnik o povredi osobnih podataka, kao i prikupiti sve dodatne relevantne dokaze i dokumentaciju. Navedeni zapisnik čini prilog ovoj Proceduri (***Prilog broj 1 – Obrazac zapisnika o povredi osobnih podataka).***

Ovisno o rezultatima naknade istrage, Agencija je dužna postupiti u skladu s pravilima o obavještavanju nadzornog tijela i ispitanika te pravilima o provođenju mjera za sprječavanje daljnjih povreda i umanjivanje posljedica nastale povrede.

XIV. VOĐENJE EVIDENCIJE NASTALIH POVREDA OSOBNIH PODATAKA

Agencija je dužna dokumentirati svaku povredu osobnih podataka, neovisno o nastalom riziku za prava i slobode ispitanika.

Agencija je dužna voditi evidenciju nastalih povreda osobnih podataka na način da kreira interni registar u elektroničkom obliku. Interni registar će se voditi na način da se za svaku nastalu povredu otvori posebna mapa čiji naziv će sadržavati vrstu povrede i datum nastanka iste.

U svaku mapu Agencija je dužna u PDF obliku (nepromjenjivom obliku) spremiti sljedeće: popunjeni i potpisani zapisnik o povredi osobnih podataka, sve relevantne dokaze i dokumentaciju u vezi povrede, službene odluke Agencije u vezi postupanja tijekom povrede, obrazloženja donesenih odluka o

postupanju u vezi povrede, popunjene obrasce o povredi i dokaz slanja istih nadzornom tijelu i ispitanicima, dokaz o javnoj objavi nastale povrede (ako je primjenjivo), svu komunikaciju s nadzornim tijelom, drugim nadležnim tijelima i ispitanicima, dokaze o poduzetim tehničkim i organizacijskim mjerama i svu ostalu dokumentaciju kojom se dokazuje postupanje Agencije u vezi nastale povrede.

Na zahtjev nadzornog i / ili drugog ovlaštenog tijela i / ili ispitanika zatražena dokumentacija se može dostaviti i u drugim traženim oblicima osim elektroničkog.

Pristup evidenciji nastalih povreda osobnih podataka mogu imati samo odgovorne osobe u Agenciji te službenik.

XV. IZVRŠITELJI OBRADE

Agencija će prilikom odabira izvršitelja obrade poduzeti sve razumne mjere da provjeri pouzdanost u odnosu na zaštitu osobnih podataka i privatnost te sigurnost obrade.

Postupanje i obveze izvršitelja obrade u slučaju povrede osobnih podataka koje on obrađuje u ime Agencije, definirat će se posebnim ugovorom o obradi osobnih podataka.

XVI. ULOGA SLUŽBENIKA

Prava i obveze službenika u slučaju nastanka povrede osobnih podataka definirane su *Pravilnikom o postupanju s osobnim podatcima* (Glavom III.) te ovom Procedurom.

Agencija je službenika dužna upoznati s odredbama *Pravilnika o postupanju s osobnim podatcima* i ovom Procedurom u svrhu poznavanja pravila u slučaju nastanka povrede osobnih podataka.

Službenik, u slučaju povrede osobnih podatka, dužan je poštivati odredbe Opće uredbe i drugih primjenjivih propisa te interna pravila propisana ovom Procedurom. Ako određena pravila propisana ovom Procedurom nisu primjenjiva na nastalu povredu osobnih podataka, službenik je dužan zatražiti uputu o postupanju od odgovorne osobe Agencije.

KLASA: 030-02/22-01/04
URBROJ: 567-10-25-3
Datum: 3. veljače 2025.

ČLAN UPRAVE

Želimir Kramarić

PREDSJEDNIK UPRAVE

Vjeran Vrbanec

Prilozi ovoj Proceduri:

- *Prilog broj 1 – Obrazac zapisnika o povredi osobnih podataka,*
- *Prilog broj 2 – Obrazac obavijesti ispitanicima o povredi osobnih podataka*