AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA • CROATIAN PERSONAL DATA PROTECTION AGENCY •

azop

ZAŠTO JE VAŽNO IMENOVATI SLUŽBENIKA ZA ZAŠTITU PODATAKA

Agencija za zaštitu osobnih podataka / Selska cesta 136 / HR – 10 000 Zagreb / e-mail: azop@azop.hr
tel.: 00385 (0)1 4609-000 / fax.: 00385 (0)1 4609-099
www.azop.hr

Zašto je važno imenovati službenika za zaštitu podataka?

DUŽNOST IMENOVANJA SLUŽBENIKA ZA ZAŠTITU PODATAKA IMAJU:

- *tijela javne vlasti*
- *organizacije koje provode redovita i sustavna praćenja u velikoj mjeri*
- *organizacije koje opsežno obrađuju posebne kategorije osobnih podataka i osobne podatake u vezi s kaznenim osudama i kažnjivim djelima (kaznene evidencije)*

> PREPORUKA

Dobrovoljno imenovati službenika, čak i kada nije propisano kao obveza.

KOJE UVJETE TREBA ISPUNJAVATI SLUŽBENIK?

- *biti lako dostupan iz svakog poslovnog nastana (kontakt točka za ispitanike, nadzorno tijelo i zaposlenike organizacije)*
- *kontakt podaci službenika trebaju biti lako dostupni (npr. objavljeni na internetskim stranicama organizacije)*
- *učinkovita komunikacija na jeziku koji upotrebljava predmetno nadzorno tijelo (AZOP) i građani*

TKO MOŽE BITI SLUŽBENIK?

- *pojedinac unutar organizacije (zaposlenik) ili*
- *vanjska organizacija (na temelju ugovora o djelu)*

> *Napomena:*
> *Skupina poduzetnika može imenovati i zajedničkog službenika.*

OSNOVNA ULOGA SLUŽBENIKA ZA ZAŠTITU PODATAKA

- *brine o tome da su poslovni procesi organizacije usklađeni s GDPR-om*
- *brine o svim pitanjima koja se odnose na zaštitu osobnih podataka u organizaciji*

VAŽNA ULOGA I NEOVISNOST SLUŽBENIKA

! *Važno: Službenik djeluje potpuno samostalno, pri čemu ne prima nikakve upute u pogledu izvršavanja svojih zadaća.*

Smjernice za zaštitu podataka je potrebno ugraditi u proizvode i usluge još u najranijim fazama razvoja.

NA KOJI NAČIN ZADOBITI POVJERENJE GRAĐANA ČIJE OSOBNE PODATKE OBRAĐUJE VAŠA ORGANIZACIJA?

- *BUDITE TRANSPARENTNI u procesima obrade osobnih podataka (primjerice putem politike privatnosti na internetskoj stranici)*
- *koristite se jednostavnim jezikom*
- *kažite im tko ste pri traženju podataka*
- *pružite informacije o njihovim pravima i načine na koje ih mogu ostvariti*
- *unaprijed informirajte zašto obrađujete njihove podatke, koliko ćete ih dugo pohranjivati, tko ih sve dobiva i sl.*

KARAKTERISTIKE KVALIFICIRANOG SLUŽBENIKA

- *profesionalne kvalitete, stručno znanje o zakonodavnom okviru i praksi iz područja zaštite podataka te sposobnost ispunjavanja zadataka službenika*

> *Kvalitetno i kontinuirano educiran službenik osigurava organizaciji prilične novčane uštede koje bi potencijalno mogle biti utrošene na podmirenje upravnih novčanih kazni zbog nepoštivanja GDPR-a.*

10 zadaća svakog službenika za zaštitu osobnih podataka

01. STVARANJE EVIDENCIJA AKTIVNOSTI OBRADE

"Evidencija je preduvjet za usklađenost te ujedno i djelotvorna mjera za osiguranje načela pouzdanosti."

Za vođenje evidencije/a aktivnosti obrade odgovoran je voditelj i/ili izvršitelj obrade.

> UPUTA

Vođenje evidencije/a aktivnosti - povjerite službeniku za zaštitu podataka.

ZAŠTO JE POTREBNO VODITI EVIDENCIJU?

- *radi dokazivanja sukladnosti s GDPR-om*
- *omogućuje obavljanje zadaća službenika u dijelu koji se odnosi na praćenje poštivanja GDPR-a*
- *smatra se i alatom koji voditelju obrade i nadzornom tijelu omogućuje da na zahtjev dobiju pregled svih aktivnosti obrade osobnih podataka koje organizacija provodi*

IZUZEĆE OD VOĐENJA EVIDENCIJA imaju poduzeća i organizacije u kojima je zaposleno manje od 250 osoba, osim ako obrada:

- *nije povremena*
- *prijetnja je pravima i slobodama pojedinaca*
- *uključuje posebne kategorije osobnih podataka ili podatke o kaznenim osudama i kažnjivim djelima*

> PREPORUKA

Voditi evidencije bez obzira na iznimke.

EVIDENCIJA TREBA SADRŽAVATI:

- *ime i kontaktne podatke organizacije*
- *svrhe obrade*
- *opis kategorija ispitanika i kategorija osobnih podataka*
- *kategorije organizacija koje primaju podatke ili će im podaci biti otkriveni*
- *prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju (ako je primjenjivo)*
- *vremenska ograničenja za uklanjanje podataka (ako je primjenjivo)*
- *opis sigurnosnih mjera koje se primjenjuju u obradi (ako je moguće)*

02. PREISPITIVANJE POSTUPAKA OBRADE

Sljedeći korak koji službenik treba poduzeti unutar svoje organizacije, a nakon kreiranja evidencija aktivnosti obrade osobnih podataka je provođenje dubinskog preispitivanja svih zabilježenih postupaka i to kako bi se provjerilo ispunjavaju li isti zahtjeve GDPR-a u svim relevantnim aspektima.

POSEBNO OBRATITI PAŽNJU NA:

- *definiranje svrhe*
- *provjera valjanosti privole (i postojanje dokumentiranog dokaza o danoj privoli) ili prihvatljivost bilo koje druge pravne osnove za obradu*
- *obrađeni osobni podaci i njihova relevantnost te nužnost u odnosu na navedenu(e) svrhu(e)*
- *točnost podataka*
- *informacije pružene ispitaniku na vlastitu inicijativu voditelja obrade – TRANSPARENTNOST*
- *definirati rok čuvanja (ukoliko nije propisan zakonom ili podzakonskim aktom)*
- *tehnička, organizacijska i fizička sigurnost podataka*
- *prekogranični prijenosi podataka (i zakonski te drugi ugovorni ili ostali dogovori u vezi istih)*

MSP-ovi trebaju voditi evidenciju samo ako je obrada podataka: redovita, potencijalna prijetnja pravima i slobodama ljudi te ako se bavi osjetljivim podacima ili kaznenim evidencijama.

OSTALA VAŽNA PITANJA ZA SAMOPROCJENU:

- *Čije i koje osobne podatke obrađuje i pohranjuje organizacija u kojoj ste službenik?*
- *Koje sustave pohrane ima?*
- *Koji je pravni temelj za obradu podataka koju provodite?*
- *Znate li u koju svrhu prikupljate i pohranjujete osobne podatke?*
- *Tko ima pravo pristupa tim podacima i tko ih koristi?*
- *Je li nužno prikupljanje tih osobnih podataka?*
- *Iznose li se podaci u treće zemlje i koja je zakonitost takvog iznošenja?*
- *Proslјeđuju li se ti podaci trećim osobama i 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/papirnatom)?*
- *Prikupljate li posebne kategorije osobnih podataka?*
- *Koji propisi reguliraju korištenje osobnih podataka?*
- *Brinete li o sigurnosti osobnih podataka?*
- *Jesu li vaši zaposlenici svjesni važnosti zaštite osobnih podataka i izjave o povjerljivosti?*
- *Jesu li tehničke mjere u skladu s člankom 32. GDPR-a i drugim povezanim člancima te posebnim propisima?*

03. PROCJENJIVANJE RIZIKA

“Podaci u svakom trenutku trebaju biti zaštićeni.“

Zadaća svakog službenika je prepoznavanje rizičnih obrada osobnih podataka kako bi mogao provesti odgovarajuće tehničke i organizacijske mjere te kako bi jamčio sigurnost osobnih podataka ili barem umanjio potencijalne rizike.

! *Važno: Potrebno je utvrditi prioritetne obrade i aktivnosti te svoj trud usmjeriti na ona pitanja koja predstavljaju veći rizik (npr. posebne kategorije podataka).*
Također, potrebno je prepoznati moguće prijetnje sigurnosti obrade te predložiti uvođenje mjera kojima će se pokušati spriječiti njihova realizacija.

Rizike koje treba procijeniti,
odnose se na vjerojatnost da će doći do:

- *povrede osobnih podataka*
- *rizika za prava i slobode pojedinaca*

Što nakon provedene procjene rizika?

Nakon što je provedena procjena, postupci obrade osobnih podataka predstavljaju rizik za relevantne interese. Stoga, službenik mora dati savjet odgovornoj osobi te predložiti ublažavanje rizika ili alternativni postupak obrade.

S CILJEM UČINKOVITOG UPRAVLJANJA RIZICIMA, A KADA JE RIJEČ O PRAVIMA I SLOBODAMA POJEDINACA,VAŽNO JE ZNATI DA RIZICI MORAJU BITI:

identificirani, analizirani, procijenjeni, tretirani (npr. ublaženi...) te redovito preispitani

04. PRUŽANJE SAVJETA PRI PROVOĐENJU PROCJENE UČINKA NA ZAŠTITU PODATAKA

U slučaju kada preliminarna procjena rizika određenog postupka obrade osobnih podataka, ukazuje na potencijalno visoki rizik za prava i slobode ispitanika, od voditelja obrade podataka se zahtijeva i očekuje provođenje procjene učinka na zaštitu podataka (DPIA) prije nastavka obrade osobnih podataka pri čemu službenik savjetuje voditelja obrade o tom postupku.

> *Primjer za ovakav slučaj može biti razvoj i primjena “nove tehnologije” u poslovanju.*

ZAŠTO PROVESTI PROCJENU UČINKA?

Jedan od značajnih alata za uspostavu i dokazivanje usklađenosti s GDPR-om.

Provođenje procjene učinka na zaštitu podataka važno je jer pomaže voditeljima obrade pri usklađivanju obrade sa zahtjevima GDPR-a te na taj način mogu dokazati da su poduzete potrebne mjere za dodatnu sigurnost obrade osobnih podataka.

Što to u praksi znači?

Voditelji obrade trebaju kontinuirano procjenjivati rizike koji potencijalno mogu nastati njihovim aktivnostima obrade i to kako bi utvrdili kada će pojedina vrsta obrade „vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca”.

05. KONTINUIRANO PREISPITIVANJE I PONAVLJANJE ANALIZA POSTUPAKA OBRADE

Službenik za zaštitu podataka pored svojih zadaća ima i dužnost praćenja poštovanja sukladnosti svoje radne organizacije s odredbama GDPR-a te bi trebao sudjelovati u procesu praćenja interne usklađenosti organizacije s GDPR-om.

> *Napomena:*
> *Izraz "praćenje" ukazuje na to da analiza stanja nije jednokratan proces već je kontinuirana odgovornost koju je potrebno periodički ponavljati*

Kada je posebno važno napraviti provjeru usklađenosti poslovanja?

Kada organizacija promijeni bilo koji postupak obrade osobnih podataka ili primijeni bilo koje nove postupke.

PREPORUKA

Službenik treba osigurati redovnu ažuriranost evidencija aktivnosti obrade.

Kada organizacija planira promjene postupaka obade, važno je provjeriti je li potrebno ažurirati evidenciju.

Preporučeno je provoditi redovite provjere, neovisno o planiranim promjenama kako bi pravodobno bile uočene promjene koje su možda ostale neprimijećene.

Kriteriji koje treba uzeti u obzir prilikom donošenja odluke o tome radi li se o obradi koja će vjerojatno prouzročiti visok rizik za prava i slobode ispitanika su:

1. *Procjena ili bodovanje, uključujući izradu profila i predviđanje*
2. *Automatizirano donošenje odluka s pravnim ili sličnim, znatnim učinkom*
3. *Sustavno praćenje obrade koja se koristi za promatranje, praćenje ili kontrolu ispitanika*
4. *Osjetljivi podaci ili podaci vrlo osobne naravi*
5. *Opsežna obrada podataka*
6. *Podudarajući ili kombinirani skupovi podataka*
7. *Podaci koji se odnose na osjetljive ispitanike*
8. *Inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja*
9. *Situacija u kojoj sama obrada sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora*

> *PRIMJER: ako tijela javne vlasti ili javna tijela namjeravaju uspostaviti zajedničku aplikaciju ili platformu za obradu ili ako nekoliko voditelja obrade namjerava uvesti zajedničku aplikaciju ili okruženje za obradu u cijeli jedan industrijski sektor ili segment ili za horizontalnu djelatnost široke uporabe.*

06. RJEŠAVANJE ZAHTJEVA ZA ZAŠTITU PRAVA POJEDINACA

Pojedinci mogu zahtijevati, primjerice:

- *informacije o tome posjedujete li njihove podatke*
- *pravo na pristup svojim osobnim podacima koje posjedujete*
- *tražiti kopiju osobnih podataka*
- *ispravak netočnih podataka (uz prilaganje točnih informacija)*
- *pravo na prenosivost podataka drugom pružatelju usluga*
- *prigovor na neku vrstu obrade osobnih podataka (npr. prestanak obrade podataka u svrhu izravnog marketinga)*
- *uputiti prigovor na automatizirano donošenje odluka*
- *brisanje osobnih podataka koje obrađujete, a koji ih se tiču*

PRAVO NA ZAŠTITU OSOBNIH PODATAKA NIJE APSOLUTNO

Pravo na zaštitu podataka je potrebno sagledati u kontekstu odnosa s drugim pravima, a testom ravnoteže ocijeniti koje pravo preteže u pojedinom slučaju.

> *ROK ZA DOSTAVU ODGOVORA -*
> *bez odgađanja, ali u svakom slučaju mjesec dana od zaprimanja zahtjeva (uz iznimke)*

07. SAVJETODAVNA ZADAĆA

Službenici moraju osigurati poštivanje GDPR-a i savjetovati voditelje obrade o ispunjavanju njihovih obveza.

U navedenom kontekstu, službenik može:

- *informirati, pružati savjete ili davati preporuke za praktično poboljšanje zaštite podataka od strane organizacije i/ili o pitanjima koja se tiču primjene odredbi o zaštiti podataka i*
- *predlagati izmjene i ažuriranja politika (pravila) i praksi organizacije vezano za zaštitu podataka u svjetlu novih pravnih instrumenata, odluka, mjera ili smjernica*

Službenik bi trebao moći pažljivo pratiti zakonodavstvo i regulatorna događanja u područjima zaštite podataka, sigurnosti podataka itd., kako bi mogao upozoriti više rangiranu upravu i relevantnu niže rangiranu upravu o:

- *nadolazećim novim EU instrumentima (kao što je Uredba o e-privatnosti) ili*
- *nove izvršne ili sudske odluke na EU-razini (kao bilo koja relevantna odluka o primjerenosti Europske komisije, koja se odnosi na treće zemlje u koje organizacija prenosi podatke, ili relevantne presude CJEU-a);*
- *nove smjernice na EU razini (bilo koja mišljenja ili preporuke, itd., koje daje Europski odbor za zaštitu podataka);*
- *i slični instrumenti, odluke, mjere ili smjernice koje su izdane u vlastitoj državi poslovnog nastana službenika (ili državama)*

> > > PREPORUKE

Što bi organizacija trebala osigurati službeniku?

Redovno sudjelovanje na sastancima višeg i srednjeg menadžmenta.

Nazočnost službenika se preporučuje kod donošenja odluka s implikacijama na zaštitu podataka.

Sve relevantne informacije je potrebno pravovremeno prenijeti službeniku kako bi se istom omogućilo stvaranje preduvjeta za pružanje adekvatnih savjeta.

Mišljenje službenika je potrebno uvažiti. U slučaju neslaganja, preporučuje se dokumentirati razloge propusta postupanja po savjetu službenika.

Službenika se treba žurno zatražiti za savjet u slučajevima kada dođe do povrede podataka ili drugih incidenata.

Kada je prikladno, voditelj ili izvršitelj obrade može izraditi smjernice za zaštitu podataka, upute ili procedure koje određuju kada i u kojim slučajevima je potrebno tražiti savjet službenika.

ŠTO ZAKLJUČITI?

Službenik je formalno zadužen za praćenje sukladnosti svih politika, izjava, pravila, ugovora i ostalih aktata kojima se uređuje zaštita osobnih podataka s GDPR-om, a koji su usvojeni ili sklopljeni od strane organizacije.

08. IZRADA INTERNIH AKATA I PROCEDURA VEZANIH UZ ZAŠTITU OSOBNIH PODATAKA

Kako bi se postigla sukladnost s GDPR-om, a posebice „dokazala“ takva sukladnost, voditelji obrade mogu i trebaju usvojiti ili se uključiti u izradu niza dokumenata odnosnih na zaštitu osobnih podataka.

DOKUMENTI KOJE BI TREBALA IMATI SVAKA „POUZDANA“ ORGANIZACIJA:

- *evidencija/e aktivnosti obrade*
- *politike (pravila) o zaštiti podataka/privatnosti (za web)*
- *interni akt za zaposlenike (Pravilnik i sl.)*
- *dogovor između zajedničkih voditelja obrade (ako je primjenjivo)*
- *ugovor između voditelja obrade i izvršitelja obrade (ako je angažiran)*
- *pravilnik o informacijskoj sigurnosti i izjave o povjerljivosti*
- *pravilnik o korištenju video nadzora*

ŠTO NAPRAVITI S POSTOJEĆIM INTERNIM DOKUMENTIMA?

- *preispitati sve postojeće dokumente i instrumente ove vrste, kako bi bilo moguće provjeriti ispunjavaju li oni i dalje u cijelosti sve pravne zahtjeve zaštite podataka*
- *temeljem takvog preispitivanja, službenik može preporučiti promjene u postojećim dokumentima, posebno ako su isti sastavljeni i usvojeni prije usvajanja i stupanja na snagu GDPR-a*
- *službenik bi trebao preporučiti i sastavljanje novih dokumenata, ako postojeći nisu zadovoljavajući*

09. DJELOVANJE KAO KONTAKTNA TOČKA

Nadzorno tijelo za zaštitu podataka u Republici Hrvatskoj je Agencija za zaštitu osobnih podataka (AZOP).

Službenik djeluje kao kontaktna točka u vidu:

- *suradnje s nadzornim tijelom i*
- *komuniciranja s pojedincima*

Navedene zadaće odnose se na njegovu ulogu „olakšavanja" obavljanja zadaća službenika u usklađivanju s odredbama GDPR-a.

Kontakt podaci stoga moraju biti jasno istaknuti na službenoj web stranici organizacije (e-mail adresa, broj telefona...).

> PREPORUKA

E-mail adresa službenika može biti i generička npr.službenik@nazivtvrtke.com međutim mora se jasno znati koja je odgovorna osoba iza toga.

10. SURADNJA S NADZORNIM TIJELOM ZA ZAŠTITU OSOBNIH PODATAKA (AZOP)

Zadaća službenika je odgovoriti na zahtjeve nadzornog tijela i surađivati s nadzornim tijelom na njegov zahtjev ili na vlastitu inicijativu.

SLUŽBENIK DJELUJE KAO:

1. KONTAKTNA TOČKA radi lakšeg pristupa dokumentima i informacijama, a radi lakšeg obavljanja zadaća AZOP-a.

2. ODGOVARA NA ZAHTJEVE AZOP-a i inicira suradnju na zahtjev tijela ili na vlastitu inicijativu.

3. PROVEDBENA FUNKCIJA – trebali bi pokušati istražiti i riješiti pritužbe na lokalnoj razini prije slanja AZOP-u.

4. MJERENJE VLASTITE UČINKOVITOSTI – smatra se korisnim alatom za samoprocjenu napretka, poticanje na razvoj vlastitih kriterija dobrog nadzora.

5. SURADNJA U VIDU PROVOĐENJA NADZORNIH AKTIVNOSTI.

Kvalitetna analiza stanja i priprema za nadzor

ANALIZA STANJA

Evidencija aktivnosti obrade
Imate li Službenika za zaštitu podataka?

Jesu li opći akti i pravilnici usklađeni s GDPR-om?
Imate li politiku privatnosti?
Primjenjujete li Izjavu o povjerljivosti?
Jesu li primijenjene odgovarajuće organizacijske i tehničke mjere zaštite osobnih podataka?

Postoji li izvršitelj obrade i jesu li ugovorom detaljno regulirana prava i obveze između voditelja i izvršitelja obrade?

Agencija za zaštitu osobnih podataka / Selska cesta 136 / HR – 10 000 Zagreb / e-mail: azop@azop.hr
tel.: 00385 (0)1 4609-000 / fax.: 00385 (0)1 4609-099
www.azop.hr

Agencija za zaštitu osobnih podataka / Selska cesta 136 / HR – 10 000 Zagreb / e-mail: azop@azop.hr
tel.: 00385 (0)1 4609-000 / fax.: 00385 (0)1 4609-099
www.azop.hr