

WP243 PRILOG – ČESTO POSTAVLJANA PITANJA

Cilj je ovog priloga na jednostavan način i u preglednom formatu odgovoriti na neka od ključnih pitanja koja organizacije mogu imati u pogledu novih zahtjeva iz Opće uredbe o zaštiti podataka za imenovanje službenika za zaštitu podataka.

Imenovanje službenika za zaštitu podataka (članak 37.)

1 Od kojih se organizacija zahtijeva imenovanje službenika za zaštitu podataka? (članak 37. stavak 1.)

Općom uredbom o zaštiti podataka zahtijeva se imenovanje službenika za zaštitu podataka u trima konkretnim slučajevima:

- ako obradu provodi tijelo javne vlasti ili javno tijelo (bez obzira na to koji se podaci obrađuju),
- ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri i
- ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka ili osobnih podataka koji se odnose na kaznene osude i kažnjiva djela.

Napominjemo da se pravom Unije ili države članice može zahtijevati imenovanje službenika za zaštitu podataka i u drugim situacijama. Međutim, ako Općom uredbom o zaštiti podataka nije izričito propisano imenovanje službenika za zaštitu podataka, za organizacije ponekad može biti korisno dobrovoljno imenovati službenika za zaštitu podataka. Radna skupina za zaštitu podataka iz članka 29. („Radna skupina iz članka 29.”) potiče takva dobrovoljna nastojanja.

Za više informacija vidjeti odjeljak 2.1. Smjernica.

2 Što znači pojam „osnovne djelatnosti”? (članak 37. stavak 1. točke (b) i (c))

„Osnovne djelatnosti” mogu se smatrati ključnim postupcima za ostvarenje ciljeva voditelja obrade ili izvršitelja obrade. One obuhvaćaju i sve djelatnosti u kojima je obrada podataka neodvojiv dio djelatnosti voditelja obrade ili izvršitelja obrade. Na primjer, obrada podataka u području zdravstva, kao što su zdravstveni kartoni pacijenata, trebala bi se smatrati jednom od osnovnih djelatnosti svake bolnice te stoga bolnice moraju imenovati službenike za zaštitu podataka.

Međutim, sve organizacije obavljaju određene pomoćne djelatnosti, na primjer plaćaju svoje zaposlenike ili osiguravaju standardnu informatičku potporu. Navedene su pomoćne funkcije nužne za osnovnu djelatnost ili osnovno poslovanje organizacije. Premda su te djelatnosti potrebne ili ključne, obično se smatraju pomoćnim funkcijama, a ne osnovnom djelatnošću.

Za više informacija vidjeti odjeljak 2.1.2. Smjernica.

3 Što znači pojam „opsežna obrada”? (članak 37. stavak 1. točke (b) i (c))

Općom uredbom o zaštiti podataka nije definirano što čini opsežnu obradu. Konkretno, Radna skupina iz članka 29. pri utvrđivanju provodi li se opsežna obrada preporučuje razmatranje sljedećih čimbenika:

- broj predmetnih ispitanika, odnosno njihov konkretan broj ili njihov udio u relevantnom stanovništvu,
- obujam podataka i/ili opseg različitih podatkovnih stavki koje se obrađuju,
- trajanje ili trajnost aktivnosti obrade podataka,
- zemljopisni razmjer aktivnosti obrade.

Primjeri opsežne obrade obuhvaćaju:

- obradu podataka o pacijentu u okviru redovnog poslovanja bolnice,
- obradu podataka o putovanjima pojedinaca koji se koriste sustavom javnog gradskog prijevoza (npr. praćenje s pomoću putnih kartica),
- obradu podataka o zemljopisnoj lokaciji klijenata međunarodnog lanca brze hrane u stvarnom vremenu u statističke svrhe koju provodi izvršitelj obrade specijaliziran za te aktivnosti,
- obradu podataka o klijentima u okviru redovnog poslovanja osiguravajućeg društva ili banke,
- obradu osobnih podataka u okviru internetske tražilice radi bihevioralnog oglašavanja,
- obradu podataka (sadržaj, promet, lokacija) koju provode pružatelji telefonskih ili internetskih usluga.

Primjeri obrade koja nije opsežna obuhvaćaju:

- obradu podataka o pacijentu koju obavlja liječnik pojedinac,
- obradu osobnih podataka koji se odnose na kaznene osude i kažnjiva djela koju obavlja odvjetnik pojedinac.

Za više informacija vidjeti odjeljak 2.1.3. Smjernica.

4 Što znači pojam „redovito i sustavno praćenje”? (članak 37. stavak 1. točka (b))

Pojam redovito i sustavno praćenje ispitanika nije definiran Općom uredbom o zaštiti podataka, ali on jasno obuhvaća sve oblike praćenja i izrade profila na internetu, uključujući i radi bihevioralnog oglašavanja. Međutim, pojam praćenja nije ograničen samo na internetsko okruženje.

Radna skupina iz članka 29. pojam „redovito praćenje” tumači na najmanje jedan od sljedećih načina:

- praćenje koje je trajno ili se provodi u određenim intervalima u određenom razdoblju,
- praćenje koje se opetovano provodi ili ponavlja u točno određeno vrijeme,
- praćenje koje se provodi stalno ili periodično.

Radna skupina iz članka 29. pojam „sustavno praćenje” tumači na najmanje jedan od sljedećih načina:

- praćenje koje se provodi u skladu s određenim sustavom,
- praćenje koje je prethodno dogovoreno, organizirano ili metodično,
- praćenje koje je dio općeg plana za prikupljanje podataka,
- praćenje koje se provodi kao dio strategije.

Primjeri: upravljanje telekomunikacijskom mrežom, pružanje telekomunikacijskih usluga, preusmjeravanje elektroničke pošte, izrada profila i ocjena radi procjene rizika (npr. radi ocjene kreditnog boniteta, određivanja premije osiguranja, sprečavanja prijevara, otkrivanja pranja novca), praćenje lokacije, na primjer s pomoću mobilnih aplikacija, programi vjernosti, bihevioralno oglašavanje, praćenje podataka o općem stanju organizma, tjelesnoj kondiciji i zdravlju s pomoću uređaja koji se nose na tijelu, televizija zatvorenog kruga, povezani uređaji, npr. pametna brojila, pametni automobili, automatizacija doma itd.

Za više informacija vidjeti odjeljak 2.1.4. Smjernica.

5 Mogu li organizacije zajednički imenovati službenika za zaštitu podataka? Ako mogu, pod kojim uvjetima? (članak 37. stavci 2. i 3.)

Općom uredbom o zaštiti podataka propisano je da skupina poduzetnika može imenovati jednog službenika za zaštitu podataka pod uvjetom da je službenik za zaštitu podataka „lako dostupan iz svakog poslovnog nastana”. Pojam dostupnosti odnosi se na zadaće službenika za zaštitu podataka kao točke za kontakt za ispitanike i nadzorno tijelo, ali i unutar organizacije. Kako bi se osiguralo da je unutarnji ili vanjski službenik za zaštitu podataka dostupan, važno je osigurati da su njegovi podaci za kontakt dostupni u skladu s Općom uredbom o zaštiti podataka. Službenik za zaštitu podataka mora moći učinkovito komunicirati s ispitanicima i surađivati s predmetnim nadzornim tijelima. To znači da se ta komunikacija mora odvijati na jeziku ili jezicima koji ili koje upotrebljavaju predmetna nadzorna tijela i ispitanici. Osobna dostupnost službenika za zaštitu podataka (bilo fizički u poslovnim prostorijama u kojima se nalaze i zaposlenici, pozivom upućenim pozivnom centru ili drugim sigurnim sredstvom komunikacije) ključna je kako bi se ispitanicima omogućilo stupanje u kontakt sa službenikom za zaštitu podataka.

Za više informacija vidjeti odjeljak 2.3. Smjernica.

6 Može li se imenovati vanjski službenik za zaštitu podataka (članak 37. stavak 6.)?

Da. U skladu s člankom 37. stavkom 6., službenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade (unutarnji službenik za zaštitu podataka) ili „obavljati zadaće na temelju ugovora o djelu”. To znači da službenik za zaštitu podataka može biti vanjski službenik te u tom slučaju svoju funkciju može obavljati na temelju ugovora o djelu sklopljenog s pojedincem ili organizacijom.

Ako je službenik za zaštitu podataka vanjski službenik, na takvog se službenika za zaštitu podataka primjenjuju svi zahtjevi iz članaka od 37. do 39. Kako je navedeno u Smjernicama, ako funkciju službenika za zaštitu podataka obavlja vanjski pružatelj usluge, jedinica koja se sastoji od pojedinaca koji rade za taj subjekt može djelotvorno provoditi zadaće službenika za zaštitu podataka kao jedinica za koju su nadležne imenovana glavna osoba za kontakt i „osoba odgovorna” za klijenta. U tom je slučaju ključno da svaki član vanjske organizacije koji obavlja funkciju službenika za zaštitu podataka ispunjava sve relevantne zahtjeve iz Opće uredbe o zaštiti podataka.

U Smjernicama se, radi pravne jasnoće i dobre organizacije, preporučuje da se u ugovor o djelu uključi jasna raspodjela zadaća u okviru vanjske jedinice službenika za zaštitu podataka te imenuje jedan pojedinac kao glavna osoba za kontakt i osoba „odgovorna” za klijenta.

Za više informacija vidjeti odjeljke 2.3., 2.4. i 3.5. Smjernica.

7 Koje bi stručne kvalifikacije trebao imati službenik za zaštitu podataka (članak 37. stavak 5.)?

Općom uredbom o zaštiti podataka propisano je da se službenik za zaštitu podataka „imenuje [...] na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz članka 39.”

Nužna razina stručnog znanja trebala bi se utvrditi u odnosu na postupke obrade podataka koji se provode te na zaštitu potrebnu za osobne podatke koji se obrađuju. Na primjer, ako je postupak obrade podataka osobito složen ili ako obuhvaća veliku količinu osjetljivih podataka, službenik za zaštitu podataka možda bi trebao imati viši stupanj stručnosti i podrške.

Potrebne vještine i stručnost podrazumijevaju:

- stručnost u pogledu nacionalnih i europskih zakona i praksi u području zaštite podataka, uključujući dubinsko razumijevanje Opće odredbe o zaštiti podataka,
- razumijevanje provedenih postupaka obrade,
- razumijevanje informacijskih tehnologija i sigurnosti podataka,
- poznavanje poslovnog sektora i organizacije,
- sposobnost promicanja kulture zaštite podataka unutar organizacije.

Za više informacija vidjeti odjeljak 2.4. Smjernica.

Radno mjesto službenika za zaštitu podataka (članak 38.)

8 Koja je sredstva potrebno pružiti službeniku za zaštitu podataka kako bi izvršavao svoje zadaće?

Člankom 38. stavkom 2. Opće uredbe o zaštiti podataka od organizacije se zahtijeva podupiranje službenika za zaštitu podataka „pružajući mu potrebna sredstva za izvršavanje [njegovih] zadaća i ostvarivanje pristupa osobnim podacima i postupcima obrade te za održavanje njegova stručnog znanja”.

Ovisno o prirodi postupaka obrade te djelatnosti i veličini organizacije službeniku za zaštitu podataka potrebno je pružiti sljedeće:

- aktivnu potporu višeg rukovodstva funkciji službenika za zaštitu podataka,
- dostatno vrijeme kako bi službenik za zaštitu podataka ispunio svoje dužnosti,
- primjerenu potporu u pogledu financijskih sredstava, infrastrukture (prostori, objekti, oprema) i, prema potrebi, osoblja,
- službenu obavijest o imenovanju službenika za zaštitu podataka upućenu svem osoblju,
- pristup ostalim službama u okviru organizacije kako bi službenik za zaštitu podataka mogao primiti nužnu potporu, doprinose ili informacije od tih službi,
- kontinuirano osposobljavanje.

Za više informacija vidjeti odjeljak 3.2. Smjernica.

9 Kojim se zaštitnim mjerama službeniku za zaštitu podataka omogućuje neovisno obavljanje zadataka (članak 38. stavak 3.)?

Uspostavljeno je nekoliko zaštitnih mjera kako bi se službeniku za zaštitu podataka omogućilo obavljanje zadataka na neovisan način, kako je navedeno u uvodnoj izjavi 97.:

- voditelj obrade ili izvršitelj obrade ne smiju službeniku za zaštitu podataka davati upute za izvršavanje zadataka,
- voditelj obrade ne smije službenika za zaštitu podataka razriješiti dužnosti ili kazniti zbog izvršavanja zadataka,
- ne smije postojati sukob interesa u odnosu na ostale moguće zadatke i dužnosti.

Za više informacija vidjeti odjeljke od 3.3. do 3.5. Smjernica.

10 Koje su „druge zadatke i dužnosti” službenika za zaštitu podataka koje mogu dovesti do sukoba interesa (članak 38. stavak 6.)?

Službenik za zaštitu podataka ne može biti djelatnik organizacije čiju svrhu i načine obrade osobnih podataka mora utvrditi. Zbog posebne organizacijske strukture svake organizacije o tomu se mora odlučivati na pojedinačnoj osnovi.

Napisano je pravilo da radna mjesta koja mogu biti u sukobu interesa mogu biti položaji u višem rukovodstvu (kao što su predsjednik uprave, direktor poslovanja, direktor financija, glavni medicinski službenik, voditelj odjela za marketing, voditelj ljudskih resursa ili voditelj odjela za informacijsku tehnologiju), ali i niže uloge u hijerarhijskoj strukturi organizacije ako takvi položaji ili uloge podrazumijevaju utvrđivanje svrhe i načina obrade osobnih podataka.

Za više informacija vidjeti odjeljak 3.5. Smjernica.

Zadaci službenika za zaštitu podataka (članak 39.)

11 Što obuhvaća pojam „praćenje poštovanja” Opće uredbe o zaštiti podataka (članak 39. stavak 1. točka (b))?

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

- prikupljati informacije radi utvrđivanja aktivnosti obrade,
- analizirati i provjeravati usklađenost aktivnosti obrade i
- obavješćivati voditelja obrade ili izvršitelja obrade te mu pružati savjete i izdavati preporuke.

Za više informacija vidjeti odjeljak 4.1. Smjernica.

12 Je li službenik za zaštitu podataka osobno odgovoran za nepoštovanje Opće uredbe o zaštiti podataka?

Ne, službenici za zaštitu podataka nisu osobno odgovorni za nepoštovanje Opće uredbe o zaštiti podataka. U Općoj uredbi o zaštiti podataka jasno je navedeno da voditelj obrade ili izvršitelj obrade mora osigurati i moći „dokazati da se obrada provodi u skladu s ovom Uredbom” (članak 24. stavak 1.). Osiguravanje usklađenosti zaštite podataka s njezinim odredbama dužnost je voditelja obrade ili izvršitelja obrade.

13 Koja je uloga službenika za zaštitu podataka u okviru procjene učinka na zaštitu podataka (članak 37. stavak 1. točka (c) i evidencije aktivnosti obrade (članak 30.)?

Kad je riječ o procjeni učinka na zaštitu podataka, voditelj obrade ili izvršitelj obrade trebali bi od službenika za zaštitu podataka zatražiti savjet u pogledu, među ostalim, sljedećih pitanja:

- provesti ili ne procjenu učinka na zaštitu podataka,
- kojom se metodologijom služiti pri provedbi procjene učinka na zaštitu podataka,
- provesti procjenu učinka na zaštitu podataka interno ili je povjeriti vanjskim izvršiteljima,
- koje zaštitne mjere (uključujući tehničke i organizacijske mjere) primijeniti radi ublaživanja mogućih rizika za prava i interese ispitanika,
- je li procjena učinka na zaštitu podataka pravilno provedena ili nije te jesu li njezini zaključci (provesti obradu ili ne te koje su zaštitne mjere primjenjive) u skladu s Općom uredbom o zaštiti podataka.

Za više informacija vidjeti odjeljak 4.2. Smjernica.

Kad je riječ o evidenciji aktivnosti obrade, voditelj obrade ili izvršitelj obrade, a ne službenik za zaštitu podataka, dužan je voditi evidenciju postupaka obrade. Međutim, ništa ne sprečava voditelja obrade ili izvršitelja obrade da službeniku za zaštitu podataka povjeri zadaću vođenja evidencije postupaka obrade za koje je odgovoran voditelj obrade. Takva bi se evidencija trebala smatrati jednim od alata koji službeniku za zaštitu podataka omogućuju obavljanje njegovih zadaća u pogledu praćenja usklađenosti, obavješćivanja i savjetovanja voditelja obrade ili izvršitelja obrade.

Za više informacija vidjeti odjeljak 4.4. Smjernica.