RADNA SKUPINA ZA ZAŠTITU PODATAKA IZ ČLANKA 29.

16/HR
WP 243 rev.01

Smjernice o službenicima za zaštitu podataka

Donesene 13. prosinca 2016.

Kako su zadnje revidirane i donesene 5. travnja 2017.

Radna skupina osnovana je na temelju članka 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnost. Njezine su zadaće opisane u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo osigurava Uprava C (Temeljna prava i vladavina prava) Europske komisije, Glavna uprava za pravosuđe i potrošače, B-1049 Bruxelles, Belgija, ured br. MO-59 03/068.

Internetska stranica: http://ec.europa.eu/justice/data-protection/index_en.htm

RADNA SKUPINA ZA ZAŠTITU POJEDINACA U VEZI S OBRADOM OSOBNIH PODATAKA

osnovana Direktivom 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995.,

uzimajući u obzir njezine članke 29. i 30.,

uzimajući u obzir njezin poslovnik,

DONIJELA JE OVE SMJERNICE:

Sadržaj

1 Uvod

Općom uredbom o zaštiti podataka („OUZP")[1] koja bi trebala stupiti na snagu 25. svibnja 2018. predviđa se uspostava osuvremenjenog okvira za usklađivanje postupaka zaštite podataka u Europi koji se temelji na pouzdanosti. Brojne će organizacije središnjom točkom tog novog pravnog okvira smatrati službenike za zaštitu podataka koji će olakšavati usklađivanje s odredbama Opće uredbe o zaštiti podataka.

U skladu s Općom uredbom o zaštiti podataka određeni voditelji obrade i izvršitelji obrade dužni su imenovati službenika za zaštitu podataka[2]. To će vrijediti za sva tijela javne vlasti i javna tijela (bez obzira na to koje podatke obrađuju) i za ostale organizacije čija je osnovna djelatnost sustavno i opsežno praćenje pojedinaca ili koje obrađuju posebne kategorije osobnih podataka u velikoj mjeri.

Čak i kad se Općom uredbom o zaštiti podataka izričito ne zahtijeva imenovanje službenika za zaštitu podataka, za organizacije ponekad može biti korisno dobrovoljno imenovanje službenika za zaštitu podataka. Radna skupina za zaštitu podataka iz članka 29. („Radna skupina iz članka 29.") potiče takva dobrovoljna nastojanja.

Pojam službenika za zaštitu podataka nije nov. Iako u skladu s Direktivom 95/46/EZ[3] organizacije nisu bile dužne imenovati službenika za zaštitu podataka, u nekoliko se država članica kroz godine svejedno razvila praksa njihova imenovanja.

Prije nego što je donesena Opća uredba o zaštiti podataka Radna skupina iz članka 29. tvrdila je da je službenik za zaštitu podataka temelj pouzdanosti i da se njegovim imenovanjem može osigurati usklađenost te da to, k tomu, može biti konkurentska prednost u poslovanju[4]. Službenici za zaštitu podataka, osim što olakšavaju usklađivanje provodeći instrumente za osiguranje pouzdanosti (kao što su olakšanje procjene učinka na zaštitu podataka i provedba ili olakšanje revizije), djeluju i kao posrednici između relevantnih dionika (npr. nadzorna tijela, ispitanici i poslovne jedinice unutar organizacija).

Službenici za zaštitu podataka nisu osobno odgovorni u slučaju neusklađenosti s Općom uredbom 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 njezinim odredbama (članak 24.

---

[1] Uredba (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 L 119, 4.5.2016.). Opća uredba o zaštiti podataka važna je za EGP i primjenjivat će se nakon što bude uključena u Sporazum o EGP-u.

[2] Službenike za zaštitu podataka dužna su imenovati i nadležna tijela su skladu s člankom 32. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.-131.) i nacionalnim provedbenim zakonodavstvom. Iako su u središtu pozornosti ovih smjernica službenici za zaštitu podataka iz Opće uredbe o zaštiti podataka, one su relevantne i za službenike za zaštitu podataka iz Direktive 2016/680 kad je riječ o sličnim odredbama.

[3] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).

[4] Vidjeti http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf.

stavak 1.). Osiguravanje usklađenosti zaštite podataka s njezinim odredbama dužnost je voditelja obrade ili izvršitelja obrade.

Osim toga, voditelj obrade ili izvršitelj obrade ima ključnu ulogu u omogućivanju djelotvornog obavljanja zadaća službenika za zaštitu podataka. Imenovanje službenika za zaštitu podataka prvi je korak, no službenicima za zaštitu podataka potrebno je isto tako dati dovoljan stupanj autonomije i dovoljno sredstava kako bi djelotvorno obavljali svoje zadaće.

U Općoj uredbi za zaštitu podataka prepoznata je ključna uloga službenika za zaštitu podataka u novom sustavu upravljanja podacima te su utvrđeni uvjeti za njegovo imenovanje, položaj i zadaće. Ovim se smjernicama nastoji objasniti relevantne odredbe Opće uredbe o zaštiti podataka kako bi se voditeljima obrade i izvršiteljima obrade pomoglo da se usklade sa zakonodavstvom, ali i kako bi se službenicima za zaštitu podataka pomoglo u njihovu radu. Smjernice sadržavaju i preporuke o najboljim praksama na temelju iskustva stečenog u određenim državama članicama EU-a. Radna skupina iz članka 29. pratit će provedbu ovih smjernica i može ih, prema potrebi, nadopuniti dodatnim pojedinostima.

2 Imenovanje službenika za zaštitu podataka

2.1. Obvezno imenovanje

Člankom 37. stavkom 1. Opće uredbe o zaštiti podataka propisano je imenovanje službenika za zaštitu podataka u trima konkretnim slučajevima[5]:

a) kada obradu provodi tijelo javne vlasti ili javno tijelo[6];
b) kada se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri; ili
c) kada se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka[7] ili[8] osobnih podataka koji se odnose na kaznene osude i kažnjiva djela[9].

U pododjeljcima u nastavku nalaze se smjernice Radne skupine iz članka 29. o kriterijima i terminologiji upotrijebljenima u članku 37. stavku 1.

Osim ako je očigledno da organizacija nije dužna imenovati službenika za zaštitu podataka, Radna skupina iz članka 29. preporučuje da voditelji obrade i izvršitelji obrade dokumentiraju interne analize provedene radi utvrđivanja je li potrebno imenovanje službenika za zaštitu podataka ili ne, kako bi mogli dokazati da su svi relevantni čimbenici primjereno uzeti u obzir[10]. Ta je analiza dio

[5] Napominjemo da se prema članku 37. stavku 4. zakonima Unije ili države članice može zahtijevati imenovanje službenika za zaštitu podataka i u drugim situacijama.
[6] Osim za sudove koji djeluju u okviru svoje sudske nadležnosti. Vidjeti članak 32. Direktive (EU) 2016/680.
[7] U skladu s člankom 9. to uključuje osobne podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obradu genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.
[8] U članku 37. stavku 1. točki (c) upotrijebljen je veznik „i”. Za objašnjenje o upotrebi veznika „ili” umjesto „i”, vidjeti odjeljak 2.1.5. u nastavku.
[9] Članak 10.
[10] Vidjeti članak 24. stavak 1.

dokumentacije prikupljene u skladu s načelom pouzdanosti. Nju bi moglo zatražiti nadzorno tijelo te bi je prema potrebi trebalo ažurirati, na primjer ako voditelji obrade ili izvršitelji obrade poduzimaju nove aktivnosti ili pružaju nove usluge s popisa slučajeva iz članka 37. stavka 1.

Ako organizacija dobrovoljno imenuje službenika za zaštitu podataka, na njegovo se imenovanje, položaj i zadaće primjenjuju zahtjevi iz članaka od 37. do 39. kao da je imenovanje bilo obvezno.

Organizaciju koja nema zakonsku obvezu imenovati službenika za zaštitu podataka i koja ga ne želi imenovati dobrovoljno ništa ne sprečava da unatoč tomu zaposli osoblje ili vanjske konzultante čije su zadaće povezane sa zaštitom osobnih podataka. U tom je slučaju važno osigurati da ne bude nejasnoća u pogledu njihovih naziva, statusa, položaja i zadaća. Zato je potrebno u svim razmjenama obavijesti unutar društva te s tijelima za zaštitu podataka, ispitanicima i širom javnošću jasno dati do znanja da naziv radnog mjesta tog pojedinca ili konzultanta nije službenik za zaštitu podataka. [11]

Službenik za zaštitu podataka imenuje se za sve postupke obrade koje obavlja voditelj obrade ili izvršitelj obrade, bez obzira na to je li njegovo imenovanje obvezno ili dobrovoljno.

2.1.1 „TIJELO JAVNE VLASTI ILI JAVNO TIJELO"

Općom uredbom o zaštiti podataka nije definiran pojam „tijelo javne vlasti ili javno tijelo". Radna skupina iz članka 29. smatra da je taj pojam potrebno odrediti u okviru nacionalnog prava. Slijedom toga, tijela javne vlasti i javna tijela uključuju nacionalna, regionalna i lokalna tijela, ali je tim pojmom u skladu s primjenjivim nacionalnim pravima obično obuhvaćen i niz drugih tijela uređenih javnim pravom[12]. U takvim je slučajevima imenovanje službenika za zaštitu podataka obvezno.

Obavljati javne zadaće i izvršavati javne ovlasti[13] mogu ne samo tijela javne vlasti i javna tijela nego i druge fizičke ili pravne osobe koje posluju u skladu s javnim pravom ili privatnim pravom u sektorima kao što su, u skladu s nacionalnim propisima svake države članice, usluge javnog prijevoza, opskrba vodom i energijom, cestovna infrastruktura, javne radiodifuzijske usluge, socijalni stanovi ili stegovna tijela za regulirane profesije.

U tim se slučajevima ispitanici mogu naći u situaciji vrlo sličnoj situaciji u kojoj njihove podatke obrađuje tijelo javne vlasti ili javno tijelo. Konkretno, podaci se mogu obrađivati za slične svrhe, a mogućnost pojedinaca da odaberu način na koji će se njihovi podaci obrađivati često je mala ili nikakva te im je zato potrebna dodatna zaštita koja se može osigurati imenovanje službenika za zaštitu podataka.

Iako u takvim slučajevima ne postoji nikakva obveza, Radna skupina iz članka 29. kao dobru praksu privatnim organizacijama koje obavljaju javne zadaće ili izvršavaju javne ovlasti preporučuje imenovanje službenika za zaštitu podataka. Djelovanje takvog službenika za zaštitu podataka

[11] To vrijedi i za službenike nadležne za zaštitu privatnosti ili druge stručnjake u području zaštite privatnosti koji danas već postoje u nekim društvima, a koji možda ne ispunjavaju kriterije predviđene Općom uredbom o zaštiti podataka, na primjer u smislu raspoloživih sredstava ili zajamčene neovisnosti pa ih se, ako te kriterije ne ispunjavaju, ne može smatrati niti nazivati službenicima za zaštitu podataka.

[12] Vidjeti, na primjer, definiciju pojmova „tijelo javnog sektora" i „tijelo uređeno javnim pravom" u članku 2. stavcima 1. i 2. Direktive 2003/98/EZ Europskog parlamenta i Vijeća od 17. studenoga 2003. o ponovnoj uporabi informacija javnog sektora (SL L 345, 31.12.2003., str. 90.).

[13] Članak 6. stavak 1. točka (e).

obuhvaća sve postupke obrade koji se provode, uključujući i one koji nisu povezani s obavljanjem javne zadaće ili izvršavanjem službene dužnosti (npr. upravljanje bazom podataka o zaposlenicima).

2.1.2 „OSNOVNE DJELATNOSTI"

Članak 37. stavak 1. točke (b) i (c) Opće uredbe o zaštiti podataka odnosi se na „osnovne djelatnosti voditelja obrade ili izvršitelja obrade". U uvodnoj izjavi 97. navodi se da „osnovne djelatnosti voditelja obrade odnose se na njegove primarne djelatnosti i ne odnose se na obradu osobnih podataka kao dodatne djelatnosti". Može se smatrati da su „osnovne djelatnosti" ključni postupci nužni za ostvarenje ciljeva voditelja obrade ili izvršitelja obrade.

Međutim, iz tumačenja pojma „osnovne djelatnosti" ne bi se smjele isključiti djelatnosti u kojima obrada podataka čini neodvojiv dio djelatnosti voditelja obrade ili izvršitelja obrade. Na primjer, osnovna djelatnost bolnice je pružanje zdravstvene skrbi. Međutim, bolnica ne bi mogla na siguran način i djelotvorno pružati zdravstvenu skrb bez obrade zdravstvenih podataka poput, na primjer, zdravstvenih kartona pacijenata. Stoga bi obradu tih podataka trebalo smatrati jednom od osnovnih djelatnosti svake bolnice i zato bolnice moraju imenovati službenike za zaštitu podataka.

Drugi je primjer privatno zaštitarsko poduzeće koje nadzire više privatnih trgovačkih centara i javnih prostora. Nadzor je osnovna djelatnost tog društva, što je pak neodvojivo povezano s obradom osobnih podataka. Zbog toga i to društvo mora imenovati službenika za zaštitu podataka.

Međutim, sve organizacije obavljaju određene djelatnosti, na primjer plaćaju svoje zaposlenike ili osiguravaju standardnu informatičku potporu. To su primjeri pomoćnih funkcija nužnih za osnovne djelatnosti ili osnovno poslovanje organizacije. Premda su te djelatnosti potrebne ili ključne, obično se smatraju pomoćnim funkcijama, a ne osnovnom djelatnošću.

2.1.3 „OPSEŽNA OBRADA"

Za aktiviranje obveze imenovanja službenika za zaštitu podataka u skladu s člankom 37. stavkom 1. točkama (b) i (c) obrada osobnih podataka koja se provodi mora biti opsežna. Općom uredbom o zaštiti podataka nije definiran izraz „opsežna obrada", iako su u uvodnoj izjavi 91. ponuđene poneke smjernice[14].

Uistinu, nije moguće brojkom koja bi bila primjenjiva u svim situacijama precizno odrediti količinu podataka koji se obrađuju ili broj pojedinih ispitanika. Time se ipak ne isključuje mogućnost da će se s

[14] Konkretno, u skladu s uvodnom izjavom bili bi uključeni postupci „obrade velikog opsega kojima se nastoji obraditi znatna količina osobnih podataka na regionalnoj, nacionalnoj ili nadnacionalnoj razini i koji bi mogli utjecati na velik broj ispitanika i koji će vjerojatno dovesti do visokog rizika, primjerice zbog osjetljivosti, u kojima se u skladu s postignutom razinom tehnološkog znanja novom tehnologijom koristi u velikom opsegu, kao i na druge postupke obrade koji dovode do visokog rizika". Međutim, u uvodnoj se izjavi izričito navodi da „obradu osobnih podataka ne bi trebalo smatrati opsežnom ako se odnosi na osobne podatke pacijenata ili klijenata pojedinih liječnika, zdravstvenih djelatnika ili odvjetnika". Važno je voditi računa o tomu da, premda su u uvodnoj izjavi navedeni primjeri krajnjih vrijednosti obujma obrade (obrada podataka koju obavlja liječnik pojedinac u usporedbi s obradom podataka iz cijele zemlje ili cijele Europe), između tih dvaju primjera postoji velika siva zona. Usto, trebalo bi imati na umu da se ta uvodna izjava odnosi na procjene učinka na zaštitu podataka. To znači da bi određeni dijelovi mogli biti svojstveni za taj kontekst i nisu nužno na isti način primjenjivi na imenovanje službenika za zaštitu podataka.

vremenom možda razviti standardna praksa za konkretnije i/ili kvantifikativno određivanje pojma „opsežna obrada" u odnosu na određene vrste uobičajenih aktivnosti obrade. Radna skupina iz članka 29. planira pridonijeti tom razvoju tako što će dijeliti i objavljivati primjere odgovarajućih pragova za aktiviranje obveze imenovanja službenika za zaštitu podataka.

U svakom slučaju, Radna skupina iz članka 29. preporučuje da se, kad se bude utvrđivalo provodi li se opsežna obrada, posebno u obzir uzmu sljedeći čimbenici:

- 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 u stvarnom vremenu u pogledu zemljopisne lokacije klijenata međunarodnog lanca brze hrane 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.

2.1.4 „REDOVITO I SUSTAVNO PRAĆENJE"

Pojam „redovito i sustavno praćenje ispitanika" u Općoj uredbi o zaštiti podataka nije definiran, ali se u uvodnoj izjavi 24.[15] spominje pojam „praćenje ponašanja ispitanika" kojim su jasno obuhvaćeni svi oblici praćenja i izrade profila na internetu, pa i za svrhe bihevioralnog oglašavanja.

Međutim, pojam praćenja nije ograničen na internetsko okruženje te bi se praćenje na internetu trebalo smatrati tek jednim od primjera praćenja ponašanja ispitanika[16].

[15] „Kako bi se odredilo može li se aktivnost obrade smatrati praćenjem ponašanja ispitanika, trebalo bi utvrditi prati li se pojedince na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova."

[16] Napominjemo da se u središtu pozornosti uvodne izjave 24. nalazi izvanteritorijalna primjena Opće uredbe o zaštiti podataka. Usto, postoji i razlika između formulacije „praćenjem njihova ponašanja" (članak 3. stavak 2.

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 djelatnosti koje se mogu smatrati redovitim i sustavnim praćenjem ispitanika: upravljanje telekomunikacijskom mrežom, pružanje telekomunikacijskih usluga, preusmjeravanje elektroničke pošte, marketinške aktivnosti temeljene na podacima, 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.

2.1.5 POSEBNE KATEGORIJE PODATAKA I PODACI KOJI SE ODNOSE NA KAZNENE OSUDE I KAŽNJIVA DJELA

U članku 37. stavku 1. točki (c) riječ je o obradi posebnih kategorija podataka na temelju članka 9. i osobnih podataka koji se odnose na kaznene osude i kažnjiva djela iz članka 10. Iako je u odredbi upotrijebljen veznik „i”, ne postoji politički razlog zbog kojeg bi ta dva kriterija trebalo primijeniti istodobno. Zato bi tekst trebalo tumačiti kao da se na tom mjestu nalazi veznik „ili”.

2.2. Službenik za zaštitu podataka izvršitelja obrade

točka (b)) i formulacije „redovito i sustavno praćenje ispitanika u velikoj mjeri” (članak 37. stavak 1. točka (b)), što se stoga može shvatiti kao različit pojam.

Kad je riječ o imenovanju službenika za zaštitu podataka, članak 37. primjenjuje se na voditelje obrade[17] i izvršitelje obrade[18]. Ovisno o tome tko ispunjava kriterije za obvezno imenovanje, u nekim je slučajevima samo voditelj obrade ili samo izvršitelj obrade dužan imenovati službenika za zaštitu podataka, dok su u ostalim slučajevima i voditelj obrade i izvršitelj obrade dužni imenovati službenika za zaštitu podataka (koji bi onda trebali međusobno surađivati).

Važno je istaknuti da čak i kad voditelj obrade ispunjava kriterije za obvezno imenovanje, to ne znači da je njegov izvršitelj obrade nužno dužan imenovati službenika za zaštitu podataka. Međutim, to bi se moglo smatrati dobrom praksom.

Primjeri:

- malo obiteljsko poduzeće koje posluje u sektoru distribucije kućanskih aparata u samo jednom gradu koristi se uslugama izvršitelja obrade čija je osnovna djelatnost pružanje usluga analize internetskih stranica i pomoći u ciljanom oglašavanju i marketingu. Djelatnosti obiteljskog poduzeća i njegovih kupaca ne iziskuju „opsežnu obradu" s obzirom na malen broj kupaca i relativno ograničenu djelatnost. Međutim, aktivnosti izvršitelja obrade, koji ima brojne klijente kao što je to malo poduzeće, sveukupno zahtijevaju obavljanje opsežne obrade. Zato izvršitelj obrade mora imenovati službenika za zaštitu podataka u skladu s člankom 37. stavkom 1. točkom (b). Istodobno, samo obiteljsko poduzeće nije dužno imenovati službenika za zaštitu podataka,

- srednje veliko proizvodno društvo podugovori usluge zaštite zdravlja na radu s vanjskim izvršiteljem obrade koji ima velik broj sličnih klijenata. Izvršitelj obrade mora imenovati službenika za zaštitu podataka na temelju članka 37. stavka 1. točke (c) pod uvjetom da se radi o opsežnoj obradi. Međutim, proizvođač nije nužno dužan imenovati službenika za zaštitu podataka.

Službenik za zaštitu podataka kojeg imenuje izvršitelj obrade nadgleda i aktivnosti organizacije koja podatke obrađuje kad djeluje samostalno kao voditelj obrade podataka (npr. ljudski resursi, informatičko poslovanje, logistika).

2.3. Imenovanje jednog službenika za zaštitu podataka za više organizacija

Člankom 37. stavkom 2. grupi poduzetnika omogućeno je imenovanje 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[19], nadzorno tijelo[20], ali i unutar organizacije s obzirom na to da je jedna od zadaća

[17] U članku 4. stavku 7. voditelj obrade definiran je kao osoba ili tijelo koje određuje svrhe i sredstva obrade.

[18] U članku 4. stavku 8. izvršitelj obrade definiran je kao osoba ili tijelo koje obrađuje osobne podatke u ime voditelja obrade.

[19] Članak 38. stavak 4.: „ispitanici se mogu obratiti službeniku za zaštitu podataka u pogledu svih pitanja povezanih s obradom svojih osobnih podataka i ostvarivanja svojih prava iz ove Uredbe".

[20] Članak 39. stavak 1. točka (e): „djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. te savjetovanje, prema potrebi, o svim drugim pitanjima".

službenika za zaštitu podataka „informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe”[21].

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 sa zahtjevima Opće uredbe o zaštiti podataka[22].

Službenik za zaštitu podataka mora biti u mogućnosti, ako je potrebno uz pomoć jedinice, učinkovito komunicirati s ispitanicima[23] i surađivati[24] s predmetnim nadzornim tijelima. To znači da se ta komunikacija mora odvijati na jeziku ili jezicima koje upotrebljavaju predmetna nadzorna tijela i ispitanici. Dostupnost službenika za zaštitu podataka (stupalo se s njim u kontakt fizički u poslovnim prostorijama u kojima se nalaze i zaposlenici, pozivom upućenim pozivnom centru ili s pomoću drugog sigurnog sredstva komunikacije) ključna je kako bi se ispitanicima omogućilo stupanje u kontakt sa službenikom za zaštitu podataka.

Na temelju članka 37. stavka 3. za nekoliko takvih vlasti ili tijela može se imenovati jedan službenik za zaštitu podataka, uzimajući u obzir njihovu organizacijsku strukturu i veličinu. Ista načela vrijede i u pogledu sredstava i komunikacije. Budući da je službenik za zaštitu podataka zadužen za niz zadaća, voditelj obrade ili izvršitelj obrade mora se pobrinuti da ih jedan službenik za zaštitu podataka, ako je potrebno uz pomoć jedinice, može obavljati učinkovito unatoč tomu što je imenovan za nekoliko tijela javne vlasti ili javnih tijela.

2.4. Dostupnost i lokacija službenika za zaštitu podataka

U skladu sa odjeljkom 4. Opće uredbe o zaštiti podataka dostupnost službenika za zaštitu podataka mora biti djelotvorna.

Kako bi se osigurala dostupnost službenika za zaštitu podataka, Radna skupina iz članka 29. preporučuje da on bude smješten u Europskoj uniji, bez obzira na to ima li voditelj obrade ili izvršitelj obrade poslovni nastan u Europskoj uniji.

Međutim, ne može se isključiti mogućnost da bi u određenim situacijama kad voditelj obrade ili izvršitelj obrade nema poslovni nastan u Europskoj uniji[25] službenik za zaštitu podataka svoju djelatnost mogao djelotvornije obavljati ako se nalazi izvan EU-a.

2.5. Stručno znanje i vještine službenika za zaštitu podataka

[21] Članak 39. stavak 1. točka (a).

[22] Vidjeti i odjeljak 2.6. u nastavku.

[23] Članak 12. stavak 1.: „Voditelj obrade poduzima odgovarajuće mjere kako bi se ispitaniku pružile sve informacije iz članaka 13. i 14. i sve komunikacije iz članaka od 15. do 22. i članka 34. u vezi s obradom u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu.”

[24] Članak 39. stavak 1. točka (d): „suradnja s nadzornim tijelom”.

[25] Vidjeti članak 3. Opće uredbe o zaštiti podataka o teritorijalnom području primjene.

Člankom 37. stavkom 5. predviđeno je sljedeće: „službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz članka 39.” Uvodnom izjavom 97. propisano da bi nužnu razinu stručnog znanja trebalo utvrditi u odnosu na postupke obrade podataka koji se provode te na obveznu zaštitu osobnih podataka koji se obrađuju.

- **Razina stručnosti**

Obvezna razina stručnosti nije strogo definirana, no ona mora biti razmjerna osjetljivosti, složenosti i količini podataka koju organizacija obrađuje. 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. Razlika postoji i ovisno o tome prenosi li organizacija sustavno podatke izvan Europske unije ili su ti prijenosi povremeni. Službenika za zaštitu podataka potrebno je odabrati pažljivo, uzimajući u obzir probleme povezane sa zaštitom podataka koji se javljaju unutar organizacije.

- **Stručne kvalifikacije**

Iako se u članku 37. stavku 5. ne navodi koje bi stručne kvalifikacije trebalo razmotriti prilikom imenovanja službenika za zaštitu podataka, neupitna je činjenica da službenici za zaštitu podataka moraju biti stručnjaci u području nacionalnog i europskog prava i prakse te dubinski razumjeti Opću uredbu o zaštiti podataka. Promidžba odgovarajućeg i redovitog osposobljavanja za službenike za zaštitu podataka koju provode nadzorna tijela svakako je od pomoći.

Korisno je i poznavanje poslovnog sektora i organizacije voditelja obrade. Službenik za zaštitu podataka mora dobro razumjeti i postupke koji se provode, informacijske sustave voditelja obrade te njegove potrebe u pogledu sigurnosti podataka i zaštite podataka.

Ako je riječ o tijelu javne vlasti ili javnom tijelu, službenik za zaštitu podataka trebao bi dobro poznavati upravna pravila i postupke te organizacije.

- **Sposobnost izvršavanja zadaća**

Sposobnost izvršavanja zadaća povjerenih službeniku za zaštitu podataka trebalo bi tumačiti u odnosu na njihove osobne kvalitete i znanja te u odnosu na njihov položaj u organizaciji. Na primjer, osobne bi kvalitete trebale obuhvaćati poštenje i visoku profesionalnu etiku. Službenik za zaštitu podataka trebao bi se prvenstveno brinuti za poštovanje Opće uredbe o zaštiti podataka. Službenik za zaštitu podataka ima ključnu ulogu u njegovanju kulture zaštite podataka unutar organizacije i pomaže u provedbi bitnih elemenata Opće uredbe o zaštiti podataka kao što su načela obrade podataka[26], prava ispitanika[27], tehnička i integrirana zaštita podataka[28], evidencija aktivnosti obrade[29], sigurnost obrade[30] te izvješćivanje i obavješćivanje o povredama podataka[31].

- **Službenik za zaštitu podataka na temelju ugovora o djelu**

Funkcija službenika za zaštitu podataka može se obavljati i na temelju ugovora o djelu sklopljenog s pojedincem ili organizacijom izvan organizacije voditelja obrade ili izvršitelja obrade. U potonjem slučaju vrlo je važno da svaki član organizacije koja izvršava funkcije službenika za zaštitu podataka ispunjava sve zahtjeve koji se primjenjuju na temelju odjeljka 4. Opće uredbe o zaštiti podataka (npr. osobito je važno da nitko ne bude u sukobu interesa). Jednako je važno da svaki član bude zaštićen odredbama Opće uredbe o zaštiti podataka (na primjer, da ne bude nepoštenog raskidanja ugovora za poslove službenika za zaštitu podataka, ali ni nepoštenog razrješenja dužnosti bilo kojeg pojedinog člana organizacije koji obavlja zadaće službenika za zaštitu podataka). Mogu se istodobno kombinirati osobne vještine i stručnost kako bi više pojedinaca koji djeluju kao jedinica mogli djelotvornije pružati usluge svojim klijentima.

U Smjernicama se, radi pravne jasnoće i dobre organizacije, preporučuje jasna raspodjela zadaća u okviru vanjske jedinice službenika za zaštitu podataka te imenovanje jednog pojedinca kao glavne osobe za kontakt i osobe „odgovorne" za klijenta. Bilo bi općenito korisno da se te stavke navedu u ugovoru o djelu.

2.6. Objava podataka za kontakt službenika za zaštitu podataka i obavješćivanje o njima

Na temelju članka 37. stavka 7. voditelj obrade ili izvršitelj objave moraju:

- objaviti podatke za kontakt službenika za zaštitu podataka i
- o podacima za kontakt službenika za zaštitu podataka obavijestiti relevantna nadzorna tijela.

Tim se zahtjevima ispitanicima (unutar i izvan organizacije) i nadzornim tijelima želi omogućiti jednostavno i izravno stupanje u kontakt sa službenikom za zaštitu podataka, a da pritom ne moraju stupiti u kontakt s nekim drugim dijelom organizacije. Jednako je važna povjerljivost: na primjer, zaposlenici mogu oklijevati u pogledu podnošenja pritužbe službeniku za zaštitu podataka ako nije zajamčena povjerljivost njihove komunikacije.
Službenik za zaštitu podataka obvezan je tajnošću ili povjerljivošću u pogledu obavljanja svojih zadaća, u skladu s pravom Unije ili pravom države članice (članak 38. stavak 5.).

[26] Poglavlje II.
[27] Poglavlje III.
[28] Članak 25.
[29] Članak 30.
[30] Članak 32.
[31] Članci 33. i 34.

Podaci za kontakt službenika za zaštitu podataka trebali bi sadržavati informacije koje će ispitanicima i nadzornim tijelima omogućiti da lako dođu do službenika za zaštitu podataka (poštanska adresa, određeni telefonski broj i/ili određena adresa elektroničke pošte). Ako je primjereno, za potrebe komuniciranja s javnošću mogu se osigurati i druga komunikacijska sredstva, na primjer za to predviđeni pozivni centar ili obrazac za kontakt koji se upućuje službeniku za zaštitu podataka na internetskoj stranici organizacije.

U skladu s člankom 37. stavkom 7. ime službenika za zaštitu podataka ne mora se navesti u objavljenim podacima za kontakt. Premda se navođenje tih podataka može smatrati dobrom praksom, voditelj obrade ili izvršitelj obrade i službenik za zaštitu podataka odlučuju je li to potrebno ili korisno u konkretnim okolnostima[32].

Međutim, ime službenika za zaštitu podataka ključno je dostaviti nadzornom tijelu kako bi službenik za zaštitu podataka mogao poslužiti kao točka za kontakt između organizacije i nadzornog tijela (članak 39. stavak 1. točka (e)).

Radna skupina iz članka 29. smatra dobrom praksom te isto tako preporučuje da organizacija svoje zaposlenike obavijesti o imenu i podacima za kontakt službenika za zaštitu podataka. Na primjer, ime i podaci za kontakt službenika za zaštitu podataka mogli bi se objaviti interno na intranetu organizacije te u internom telefonskom imeniku i organigramima.

3 Radno mjesto službenika za zaštitu podataka

3.1. Sudjelovanje službenika za zaštitu podataka u svim pitanjima koja se odnose na zaštitu osobnih podataka

Člankom 38. Opće uredbe o zaštiti podataka propisano je da voditelj obrade i izvršitelj obrade osiguravaju da je službenik za zaštitu podataka „na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka”.

Vrlo je važno da službenik za zaštitu podataka ili njegova jedinica bude što ranije uključeni u sva pitanja koja se odnose na zaštitu podataka. U pogledu procjene učinka na zaštitu podataka, Općom uredbom o zaštiti podataka izričito se predviđa rano uključivanje službenika za zaštitu podataka te se navodi da pri provedbi procjene učinka na zaštitu podataka voditelj obrade traži savjet službenika za zaštitu podataka[33]. Ako se osigura obavješćivanje službenika za zaštitu podataka i savjetovanje s njim od samoga početka, olakšat će se usklađivanje s Općom uredbom o zaštiti podataka i promicati pristup integrirane zaštite privatnosti, i zato bi to trebalo biti dio uobičajenog upravljanja organizacijom. Povrh toga, važno je da je službenik za zaštitu podataka u organizaciji prihvaćen kao partner u raspravi te da bude dio relevantnih radnih skupina koje se unutar organizacije bave poslovima obrade podataka.

[32] Valja primijetiti da se u članku 33. stavku 3. točki (b), u kojoj se opisuju informacije koje je potrebno pružiti nadzornom tijelu i ispitanicima u slučaju povrede osobnih podataka, za razliku od članka 37. stavka 7., izričito zahtijeva da se navede ime (a ne samo podaci za kontakt) službenika za zaštitu podataka.
[33] Članak 35. stavak 2.

Slijedom toga, organizacija bi se, na primjer, trebala pobrinuti:

- da je službenik za zaštitu podataka pozvan sudjelovati na redovitim sastancima visokog i srednjeg rukovodstva,
- da se preporuči nazočnost službenika za zaštitu podataka kad se donose odluke koje se mogu odraziti na zaštitu podataka. Sve se relevantne informacije službeniku za zaštitu podataka moraju proslijediti pravodobno kako bi mogao pružiti odgovarajući savjet,
- da se mišljenje službenika za zaštitu podataka uvijek uzme u obzir. U slučaju neslaganja, Radna skupina iz članka 29. smatra dobrom praksom i preporučuje da se zabilježe razlozi zbog kojih se nije slijedio savjet službenika za zaštitu podataka,
- da se savjetovanje sa službenikom za zaštitu podataka provede odmah nakon što je došlo do povrede podataka ili do nekog drugog incidenta.

Prema potrebi, voditelj obrade ili izvršitelj obrade može izraditi smjernice za zaštitu podataka ili programe u kojima je propisano kad je savjetovanje sa službenikom za zaštitu podataka obvezno.

3.2. Potrebna sredstva

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”. Osobito valja razmotriti sljedeće stavke:

- aktivnu potporu visokog rukovodstva (na razini upravnog odbora) funkciji službenika za zaštitu podataka,
- da se službenicima za zaštitu podataka osigura dovoljno vremena za ispunjavanje njihovih zadaća. To je osobito važno kad imenovani interni službenik za zaštitu podataka ne radi puno radno vrijeme ili kad vanjski službenik za zaštitu podataka obavlja poslove zaštite podataka povrh ostalih dužnosti. U suprotnom bi, zbog sukobljenih prioriteta, dužnosti službenika za zaštitu podataka mogle biti zanemarene. Od najveće je važnosti posvetiti dovoljno vremena obavljanju zadaća službenika za zaštitu podataka. Dobra je praksa utvrditi postotak vremena predviđen za obavljanje dužnosti službenika za zaštitu podataka ako se ona ne obavlja u punom radnom vremenu. Dobra je praksa odrediti i vrijeme potrebno za obavljanje te dužnosti, odgovarajuću razinu prioritetnosti pojedinih zadaća službenika za zaštitu podataka te izraditi plan rada za službenika za zaštitu podataka (ili za organizaciju),
- da se osigura odgovarajuća potpora u smislu financijskih sredstava, infrastrukture (poslovni prostori, objekti, oprema) i, prema potrebi, osoblja,
- da se svem osoblju dostavi službena obavijest o imenovanju službenika za zaštitu podataka kako bi se osiguralo da su u organizaciji svi upoznati s njegovim postojanjem i dužnostima,
- da se omogući nužan pristup ostalim službama, kao što su ljudski resursi, pravna služba, informacijske tehnologije, sigurnost itd., kako bi službenici za zaštitu podataka od tih službi mogli dobivati neophodnu potporu, doprinose i informacije,
- da se omogući kontinuirano osposobljavanje. Službenik za zaštitu podataka mora imati priliku upoznavati se s novim otkrićima u području zaštite podataka. Trebalo bi stremiti ka stalnom unapređivanju razine stručnosti službenika za zaštitu podataka te bi ih trebalo poticati da pohađaju tečajeve osposobljavanja o zaštiti podataka i druge oblike stručnog usavršavanja kao što je sudjelovanje na forumima i radionicama o zaštiti privatnosti itd.,

- s obzirom na veličinu i ustroj organizacije, moglo bi biti potrebno uspostaviti jedinicu službenika za zaštitu podataka (službenik za zaštitu podataka i njegova jedinica). U takvim je slučajevima potrebno jasno izraditi plan unutarnjeg ustroja jedinice te zadaće i odgovornosti svakog njezina člana. Slično tomu, ako dužnost službenika za zaštitu podataka izvršava vanjski pružatelj usluga, jedinica koja se sastoji od pojedinaca koji rade za taj poslovni subjekt može djelotvorno obavljati zadaće službenika za zaštitu podataka kao jedinica pod odgovornošću imenovane glavne osobe za kontakt za tog klijenta.

Uglavnom, što su složeniji i/ili osjetljiviji postupci obrade, to službeniku za zaštitu podataka treba dati više sredstava. Obavljanje dužnosti zaštite podataka mora biti djelotvorno te za nju moraju postojati dostatna sredstva s obzirom na obradu podataka koju obuhvaća.

3.3. Davanje uputa i „obavljanje svoje dužnosti i zadaća na neovisan način"

Člankom 38. stavkom 3. uspostavljena su određena osnovna jamstva kao pomoć da se službenicima za zaštitu podataka osigura mogućnost da svoje zadaće obavljaju s dovoljnim stupnjem autonomije. Konkretno, od voditelja obrade/izvršitelja obrade zahtijeva se da osiguraju da službenik za zaštitu podataka „ne prima nikakve upute u pogledu izvršenja [svojih] zadaća". U uvodnoj izjavi 97. još je navedeno da bi službenici za zaštitu podataka, „bez obzira jesu li zaposlenici voditelja obrade, trebali [...] moći obavljati svoje dužnosti i zadaće na neovisan način".

To znači da se službenicima za zaštitu podataka koji ispunjavaju svoje zadaće u skladu s člankom 39. ne smiju davati upute o načinu rješavanja predmeta, na primjer, o ishodu koji bi trebalo ostvariti, načinu vođenja istrage o pritužbi ili o tomu treba li tražiti savjet nadzornog tijela. Nadalje, ne smije ih se uputiti da zauzmu određeno stajalište o predmetu koji se odnosi na zakon o zaštiti podataka, na primjer, na određeno tumačenje zakona.

Ipak, to što službenici za zaštitu podataka svoje zadaće obavljaju autonomno ne znači da njihove ovlasti odlučivanja premašuju njihove zadaće na temelju članka 39.

Voditelj obrade ili izvršitelj obrade i dalje je odgovoran za usklađenost s pravom u području zaštite podataka i tu usklađenost mora biti u mogućnosti dokazati[34]. Ako voditelj obrade ili izvršitelj obrade donese odluke nespojive s Općom uredbom o zaštiti podataka i savjetom službenika za zaštitu podataka, službeniku za zaštitu podataka trebalo bi omogućiti da svoje suprotno mišljenje jasno da do znanja najvišoj rukovodećoj razini te onima koji donose odluke. U tom pogledu člankom 38. stavkom 3. predviđeno je da službenik za zaštitu podataka „izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade". Takvim izravnim odgovaranjem najvišoj rukovodećoj razini osigurava se da najviše rukovodstvo (npr. uprava) bude obaviješteno o tome koji je savjet i koje preporuke službenik za zaštitu podataka dao u okviru svoje zadaće informiranja i savjetovanja voditelja obrade ili izvršitelja obrade. Sastavljanje godišnjeg izvješća o aktivnostima službenika za zaštitu podataka koje se dostavlja najvišoj rukovodećoj razini još je jedan primjer izravnog odgovaranja najvišoj rukovodećoj razini.

3.4. Razrješenje dužnosti ili kazna zbog izvršavanja zadaća službenika za zaštitu podataka

[34] Članak 5. stavak 2.

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

Tom se odredbom pojačava autonomija službenika za zaštitu podataka te se pomaže osigurati neovisnost njihova djelovanja i njihova dostatna zaštita pri obavljanju svojih zadaća zaštite podataka.

Na temelju Opće uredbe o zaštiti podataka kažnjavanje je zabranjeno samo ako su kazne uvedene zbog posljedice nastale zato što je službenik za zaštitu podatka obavljao svoje zadaće. Na primjer, službenik za zaštitu podataka može smatrati da će određena obrada vjerojatno izazvati visok stupanj rizika i savjetuje voditelju obrade ili izvršitelju obrade da provede ocjenu učinka na zaštitu podataka, no voditelj obrade ili izvršitelj obrade ne slaže se s tom procjenom službenika za zaštitu podataka. Službenika za zaštitu podataka u toj se situaciji ne može razriješiti dužnosti samo zato što je ponudio taj savjet.

Kazne mogu biti raznolike te izravne i neizravne. Na primjer, mogu se sastojati od izostanka ili odgode promaknuća; onemogućenog napredovanja u karijeri; uskraćivanja pogodnosti koje dobivaju ostali zaposlenici. Te kazne ne moraju nužno biti provedene, već je i sama prijetnja kaznom dovoljna ako se njome službenik za zaštitu podataka kažnjava u pogledu njegovih aktivnosti u ulozi službenika za zaštitu podataka.

Uvriježeno je pravilo upravljanja, koje je ujedno primjenjivo i na bilo kojeg drugog zaposlenika ili nositelja ugovora kojeg obuhvaća i na kojeg se odnosi nacionalno ugovorno ili radno i kazneno pravo, da službenik za zaštitu podataka može ipak zakonito biti razriješen dužnosti zbog razloga koji nisu povezani s izvršavanjem njegovih zadaća službenika za zaštitu podataka (na primjer, u slučaju krađe, fizičkog, psihičkog ili spolnog uznemiravanja ili slične grube povrede dužnosti).

U tom je kontekstu potrebno napomenuti da se Općom uredbom o zaštiti podataka ne propisuje kako i kada se službenik za zaštitu podataka može razriješiti dužnosti ili zamijeniti drugom osobom. Međutim, što je stabilniji ugovor o radu službenika za zaštitu podataka i što je više jamstava da neće biti nepoštenog razrješenja dužnosti, to je izglednije da će službenici za zaštitu podataka moći djelovati na neovisan način. Zbog toga bi Radna skupina iz članka 29. pozdravila napore organizacije s tim ciljem.

3.5. Sukob interesa

U skladu s člankom 38. stavkom 6. službenik za zaštitu podataka „može ispunjavati i druge zadaće i dužnosti”. Tim se člankom, međutim, zahtijeva da organizacija osigura da „takve zadaće i dužnosti ne dovedu do sukoba interesa”.

Nepostojanje sukoba interesa usko je povezano s obvezom djelovanja na neovisan način. Iako je službenicima za zaštitu podataka dopušteno obavljati druge dužnosti, te im druge zadaće i obveze mogu biti povjerene samo uz uvjet da ne dovode do sukoba interesa. Konkretno, to podrazumijeva da 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.

Nepisano je pravilo da radna mjesta koja mogu biti u sukobu interesa u okviru organizacije 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. Osim toga, sukob interesa može nastati, na primjer, ako se od vanjskog službenika za zaštitu podataka zatraži da pred sudovima predstavlja voditelja obrade ili izvršitelja obrade u slučajevima koji uključuju pitanja zaštite podataka.

Ovisno o djelatnostima, veličini i strukturi organizacije, za voditelje obrade ili izvršitelje u praksi bi moglo biti dobro sljedeće:

- utvrditi funkcije koje su nespojive s funkcijom službenika za zaštitu podataka,
- sastaviti interna pravila za tu svrhu kako bi se izbjegao sukob interesa,
- dodati i šire objašnjenje o sukobu interesa,
- izjaviti da njihov službenik za zaštitu podataka nije u sukobu interesa s obzirom na njegovu dužnost službenika za zaštitu podataka, što će pridonijeti podizanju svijesti o postojanju te obveze,
- u interna pravila organizacije uvrstiti zaštitne mjere i osigurati da je natječaj za radno mjesto službenika za zaštitu podataka ili ugovor o djelu dostatno precizan i iscrpan radi izbjegavanja sukoba interesa. U tom bi kontekstu trebalo imati na umu da se sukobi interesa mogu pojaviti u raznim oblicima, ovisno o tome je li službenik za zaštitu podataka već bio zaposlenik organizacije ili nije.

4 Zadaće službenika za zaštitu podataka

4.1. Praćenje usklađenosti s Općom uredbom o zaštiti podataka

Člankom 39. stavkom 1. točkom (b) službenicima za zaštitu podataka povjerava se, među ostalim, zadaća praćenja poštovanja Opće uredbe o zaštiti podataka. U uvodnoj izjavi 97. dodatno se precizira da bi službenik za zaštitu podataka trebao „pomagati voditelju obrade ili izvršitelju obrade pri praćenju unutarnje usklađenosti s ovom Uredbom”.

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.

To što službenik za zaštitu podataka prati usklađenost ne znači da je on osobno odgovoran u slučaju pojave neusklađenosti. U Općoj uredbi o zaštiti podataka jasno se daje do znanja da je voditelj obrade, a ne službenik za zaštitu podataka, taj koji obvezno „provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom” (članak 24. stavak 1.). Usklađenost u području zaštite podataka korporativna je odgovornost voditelja obrade, a ne službenika za zaštitu podataka.

4.2. Uloga službenika za zaštitu podataka u procjeni učinka na zaštitu podataka

Na temelju članka 35. stavka 1. voditelj obrade, a ne službenik za zaštitu podataka, dužan je, prema potrebi, provesti procjenu učinka na zaštitu osobnih podataka. Međutim, službenik za zaštitu podataka može imati vrlo važnu i korisnu ulogu u pružanju pomoći voditelju obrade.. Slijedom načela integrirane zaštite podataka, člankom 35. stavkom 2. izričito se zahtijeva da voditelj obrade „traži savjet" od službenika za zaštitu podataka pri provedbi procjene učinka na zaštitu podataka. Člankom 39. stavkom 1. točkom (c) obvezuje se pak službenika za zaštitu podataka na „pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35."

Radna skupina iz članka 29. preporučuje da voditelj obrade traži savjet od službenika za zaštitu podataka u pogledu, među ostalim, sljedećih pitanja [35]:

- 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 ublažavanja 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.

Ako voditelj obrade nije suglasan sa savjetom službenika za zaštitu podataka, u dokumentaciji o procjeni učinka na zaštitu podataka potrebno je u pisanom obliku konkretno obrazložiti zašto savjet nije uzet u obzir[36].

Radna skupina iz članka 29. nadalje preporučuje da voditelj obrade, na primjer, u ugovoru službenika za zaštitu podataka te u informacijama koje se dostavljaju zaposlenicima, rukovoditeljima (i ostalim dionicima, prema potrebi) jasno navede točne zadaće službenika za zaštitu podataka i njihov opseg, osobito u pogledu provedbe procjene učinka na zaštitu podataka.

4.3. Suradnja s nadzornim tijelima i djelovanje kao točka za kontakt

U skladu s člankom 39. stavkom 1. točkama (d) i (e), zadaće koje bi službenik za zaštitu podataka trebao obavljati su „suradnja s nadzornim tijelom" i „djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. te savjetovanje, prema potrebi, o svim drugim pitanjima".

Te se zadaće odnose na njegovu ulogu „olakšavanja" obavljanja zadaća službenika za zaštitu podataka o kojoj je bilo riječi u uvodnom dijelu ovih Smjernica. Službenik za zaštitu podataka djeluje kao točka za kontakt koja nadzornom tijelu olakšava pristup dokumentima i informacijama za obavljanje zadaća iz članka 57. te izvršavanje njegovih istražnih ovlasti, korektivnih ovlasti, ovlasti povezanih s

[35] U članku 39. stavku 1. spominju se zadaće službenika za zaštitu podataka te se navodi da on ima „najmanje" sljedeće zadaće. Stoga voditelja obrade ništa ne sprečava da službeniku za zaštitu podataka dodijeli druge zadaće osim onih izričito navedenih u članku 39. stavku 1. ili da ih podrobno objasni.

[36] Člankom 24. stavkom 1. predviđa se da „uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i **mogao dokazati** da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju".

odobravanjem i savjetodavnih ovlasti navedenih u članku 58. Kao što je prethodno već navedeno, službenik za zaštitu podataka obvezan je tajnošću ili povjerljivošću u vezi s obavljanjem svojih zadaća, u skladu s pravom Unije ili pravom države članice (članak 38. stavak 5.). Međutim, obveza čuvanja tajnosti/povjerljivosti ne znači da je službeniku za zaštitu podataka zabranjeno obratiti se nadzornom tijelu i od njega zatražiti savjet. U skladu s člankom 39. stavkom 1. točkom (e) službenik za zaštitu podataka može se, prema potrebi, savjetovati s nadzornim tijelom o svim ostalim pitanjima.

4.4. Pristup temeljen na riziku

Člankom 39. stavkom 2. zahtijeva se da službenik za zaštitu podataka „vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade".

U tom se članku podsjeća na opće zdravorazumsko načelo koje bi se moglo primijeniti na brojne aspekte svakodnevnog rada službenika za zaštitu podataka. Njime se, u biti, od službenika za zaštitu podataka zahtijeva da utvrde prioritetne aktivnosti i svoj trud usmjere na pitanja koja predstavljaju veći rizik za zaštitu podataka. To ne znači da bi trebali zanemariti praćenje usklađenosti postupaka obrade podataka koje obilježava niža razina rizika u odnosu na pitanja koja obilježava viša razina rizika, ali upućuje na to da bi u središtu pozornosti prvenstveno trebala biti područja višeg rizika.

Takav bi selektivan i pragmatičan pristup službenicima za zaštitu podataka trebao pomoći da voditeljima obrade pruže savjete o tomu koju metodologiju upotrijebiti za provedbu procjene učinka na zaštitu podataka, koja bi područja trebalo podvrgnuti unutarnjoj i vanjskoj reviziji zaštite podataka, koje interne aktivnosti osposobljavanja osigurati za osoblje ili rukovoditelje odgovorne za aktivnosti obrade podataka i kojim radnjama obrade posvetiti više svojeg vremena i sredstava.

4.5. Uloga službenika za zaštitu podataka u vođenju evidencije

U skladu s člankom 30. stavcima 1. i 2. voditelj obrade ili izvršitelj obrade, a ne službenik za zaštitu podataka, „vodi evidenciju aktivnosti obrade za koje je odgovoran" ili „vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju za voditelja obrade".

Službenici za zaštitu podataka u praksi često sastavljaju popise i vode evidenciju postupaka obrade na temelju informacija koje su im dostavili različiti odjeli u njihovoj organizaciji odgovorni za obradu osobnih podataka. Ta je praksa uspostavljena u okviru brojnih postojećih nacionalnih propisa i u skladu s pravilima za zaštitu podataka koja se primjenjuju na institucije i tijela EU-a[37].

U članku 39. stavku 1. naveden je popis zadaća službenika za zaštitu podataka čije se obavljanje smatra minimumom. Stoga voditelja obrade ili izvršitelja obrade ništa ne sprečava da službeniku za zaštitu podataka dodijeli zadaću vođenja evidencije postupaka obrade za koje je odgovoran voditelj obrade ili izvršitelj 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.

U svakom slučaju, evidenciju koja se obvezno vodi na temelju članka 30. trebalo bi smatrati i alatom koji voditelju obrade i nadzornom tijelu omogućuje da na zahtjev dobiju pregled svih aktivnosti obrade osobnih podataka koje organizacija provodi. Ona je stoga preduvjet za usklađenost i, kao takva, djelotvorna mjera za osiguranje načela pouzdanosti.

[37] Članak 24. stavak 1. točka (d) Uredbe (EZ) 45/2001.

5 PRILOG – SMJERNICE SLUŽBENIKA ZA ZAŠTITU PODATAKA: ŠTO TREBATE ZNATI

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

1 Od kojih se organizacija zahtijeva imenovanje službenika za zaštitu podataka?

Imenovanje službenika za zaštitu podataka obvezno je:

- 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,
- 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 imenovanje službenika za zaštitu podataka nije obvezno, 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. Ako organizacija dobrovoljno imenuje službenika za zaštitu podataka, na njegovo se imenovanje, položaj i zadaće primjenjuju isti zahtjevi kao da je imenovanje bilo obvezno.

Izvor: članak 37. stavak 1. Opće uredbe o zaštiti podataka

2 Što znači pojam „osnovne djelatnosti”?

„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. To su primjeri pomoćnih funkcija nužnih za osnovne djelatnosti ili osnovno poslovanje organizacije. Premda su te djelatnosti potrebne ili ključne, obično se smatraju pomoćnim funkcijama, a ne osnovnom djelatnošću.

Izvor: članak 37. stavak 1. točke (b) i (c) Opće uredbe o zaštiti podataka

3 Što znači pojam „opsežna obrada”?

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.

Izvor: članak 37. stavak 1. točke (b) i (c) Opće uredbe o zaštiti podataka

4 Što znači pojam „redovito i sustavno praćenje”?

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.

Primjeri djelatnosti koje se mogu smatrati redovitim i sustavnim praćenjem ispitanika: upravljanje telekomunikacijskom mrežom, pružanje telekomunikacijskih usluga, preusmjeravanje elektroničke pošte, marketinške aktivnosti temeljene na podacima, 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.

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.

Izvor: članak 37. stavak 1. točka (b) Opće uredbe o zaštiti podataka

5 Mogu li organizacije zajednički imenovati službenika za zaštitu podataka? Ako mogu, pod kojim uvjetima?

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. Službenik za zaštitu podataka mora moći, ako je potrebno uz pomoć jedinice, 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. Dostupnost službenika za zaštitu podataka (stupalo se s njim u kontakt fizički u poslovnim prostorijama u kojima se nalaze i zaposlenici, pozivom upućenim pozivnom centru ili s pomoću drugog sigurnog sredstva komunikacije) ključna je kako bi se ispitanicima omogućilo stupanje u kontakt sa službenikom za zaštitu podataka.

Za nekoliko tijela javne vlasti ili javnih tijela može se imenovati jedan službenik za zaštitu podataka, uzimajući u obzir njihovu organizacijsku strukturu i veličinu. Ista načela vrijede i u pogledu sredstava i komunikacije. Budući da je službenik za zaštitu podataka zadužen za čitav niz zadaća, voditelj obrade ili izvršitelj obrade mora se pobrinuti da ih jedan službenik za zaštitu podataka, ako je potrebno uz pomoć jedinice, može obavljati učinkovito unatoč tomu što je imenovan za nekoliko tijela javne vlasti ili javnih tijela.

Izvor: članak 37. stavci 2. i 3. Opće uredbe o zaštiti podataka

6 Gdje bi se službenik za zaštitu podataka trebao nalaziti?

Kako bi se osigurala dostupnost službenika za zaštitu podataka, Radna skupina iz članka 29. preporučuje da on bude smješten u Europskoj uniji, bez obzira na to ima li voditelj obrade ili izvršitelj obrade poslovni nastan u Europskoj uniji. Međutim, ne može se isključiti mogućnost da bi u određenim situacijama kad voditelj obrade ili izvršitelj obrade nema poslovni nastan u Europskoj uniji službenik za zaštitu podataka svoju djelatnost mogao djelotvornije obavljati ako se nalazi izvan EU-a.

7 Je li moguće imenovati vanjskog službenika za zaštitu podataka?

Da. Službenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade (interni 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 funkciju službenika za zaštitu podataka izvršava vanjski pružatelj usluga, jedinica koja se sastoji od pojedinaca koji rade za taj poslovni subjekt može djelotvorno obavljati zadaće službenika za zaštitu podataka kao jedinica pod odgovornošću imenovane glavne osobe za kontakt i „osobe odgovorne" za klijenta. U tom je slučaju bitno da svaki član vanjske organizacije koja izvršava funkcije službenika za zaštitu podataka ispunjava relevantne zahtjeve iz Opće uredbe za zaštitu 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.

Izvor: članak 37. stavak 6. Opće uredbe o zaštiti podataka

8 Koje bi stručne kvalifikacije trebao imati službenik za zaštitu podataka?

Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja njegovih zadaća.

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.

Izvor: članak 37. stavak 5. Opće uredbe o zaštiti podataka

Radno mjesto službenika za zaštitu podataka

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

Službenik za zaštitu podataka mora raspolagati sredstvima potrebnim za izvršavanje svojih zadaća.

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.

Izvor: članak 38. stavak 2. Opće uredbe o zaštiti podataka

10 Kojim se zaštitnim mjerama službeniku za zaštitu podataka omogućuje neovisno obavljanje zadataka? Što znači izraz „sukob interesa”?

Uspostavljeno je nekoliko zaštitnih mjera kako bi se službeniku za zaštitu podataka omogućilo obavljanje zadaća na neovisan način:

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

Ostale zadaće i dužnosti službenika za zaštitu podataka ne smiju za posljedicu imati sukob interesa. To ponajprije znači 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.

Nepisano je pravilo da radna mjesta koja mogu biti u sukobu interesa u okviru organizacije 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. Osim toga, sukob interesa može nastati, na primjer, ako se od vanjskog službenika za zaštitu podataka zatraži da pred sudovima predstavlja voditelja obrade ili izvršitelja obrade u slučajevima koji uključuju pitanja zaštite podataka.

Izvor: članak 38. stavak 3. i članak 38. stavak 6. Opće uredbe o zaštiti podataka

Zadaće službenika za zaštitu podataka

11 Što znači izraz „praćenje poštovanja”?

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.

Izvor: članak 39. stavak 1. točka (b) Opće uredbe o zaštiti podataka

12 Je li službenik za zaštitu podataka osobno odgovoran za nepoštovanje zahtjeva za zaštitu podataka?

Ne. Službenici za zaštitu podataka nisu osobno odgovorni za nepoštovanje zahtjeva za zaštitu podataka. Voditelj obrade ili izvršitelj obrade mora osigurati i moći dokazati da se obrada provodi u skladu s Uredbom. 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 i evidencije aktivnosti obrade?

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 ublažavanja 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 sa zahtjevima za zaštitu podataka.

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 ili izvršitelj 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.

Izvor: članak 39. stavak 1. i članak 30. Opće uredbe o zaštiti podatka

Sastavljeno u Bruxellesu 13. prosinca 2016.

Za Radnu skupinu,
Predsjednica

Isabelle FALQUE-PIERROTIN

Kako su zadnje revidirane i donesene 5. travnja 2017.

Za Radnu skupinu
Predsjednica

Isabelle FALQUE-PIERROTIN