

PRILOGA K DOKUMENTU WP243 – POGOSTO ZASTAVLJENA VPRAŠANJA

Cilj te priloge je v poenostavljeni in lahko berljivi obliki odgovoriti na nekatera ključna vprašanja, ki bi jih utegnile imeti organizacije v zvezi z novimi zahtevami iz Splošne uredbe o varstvu podatkov glede imenovanja pooblaščenih oseb za varstvo podatkov.

Imenovanje pooblaščenih oseb za varstvo podatkov (člen 37)

1 Katere organizacije morajo imenovati pooblaščenih osebo za varstvo podatkov? (člen 37(1))

V skladu s Splošno uredbo o varstvu podatkov je treba pooblaščenih osebo za varstvo podatkov imenovati v treh posebnih primerih:

- kadar obdelavo opravlja javni organ ali telo (ne glede na to, kateri podatki se obdelujejo);
- kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba posameznike, na katere se nanašajo osebni podatki, redno in sistematično obsežno spremljati, in.
- kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

Upoštevati je treba, da lahko pravo Unije ali države članice imenovanje pooblaščenih oseb za varstvo podatkov zahteva tudi v drugih primerih. Kadar Splošna uredba o varstvu podatkov ne zahteva izrecno imenovanja pooblaščenih oseb za varstvo podatkov, se včasih organizacijam lahko zdi koristno, da pooblaščenih osebo za varstvo podatkov imenujejo prostovoljno. Delovna skupina za varstvo podatkov iz člena 29 (v nadaljnjem besedilu: delovna skupina iz člena 29) spodbuja ta prostovoljna prizadevanja.

Več informacij je na voljo v oddelku 2.1 smernic.

2 Kaj pomeni pojem „temeljne dejavnosti“? (člen 37(1)(b) in (c))

Za „temeljne dejavnosti“ se lahko štejejo dejavnosti, ki so ključne za doseganje ciljev upravljavca ali obdelovalca. Vključujejo tudi vse dejavnosti, pri katerih je obdelava podatkov neločljiv del dejavnosti upravljavca ali obdelovalca. Na primer obdelavo zdravstvenih podatkov, kot je zdravstvena dokumentacija bolnikov, bi bilo treba obravnavati kot eno od temeljnih dejavnosti vseh bolnišnic, ki morajo zato imenovati pooblaščenih osebe za varstvo podatkov.

Na drugi strani vse organizacije izvajajo nekatere podporne dejavnosti, na primer plačevanje zaposlenih ali standardne dejavnosti informacijske podpore. To so potrebne podporne funkcije za temeljno ali glavno dejavnost organizacije. Čeprav so te dejavnosti potrebne ali nujne, se navadno štejejo za pomožne funkcije in ne temeljne dejavnosti.

Več informacij je na voljo v oddelku 2.1.2 smernic.

3 Kaj pomeni pojem „obsežno“? (člen 37(1)(b) in (c))

Splošna uredba o varstvu podatkov ne opredeljuje, kaj je obsežno. Delovna skupina iz člena 29 priporoča, da se pri določanju, ali je obdelava obsežna, upoštevajo zlasti naslednji dejavniki:

- število zadevnih posameznikov, na katere se nanašajo osebni podatki – bodisi kot določeno število ali delež ustrezne populacije;
- količina podatkov in/ali razpon različnih podatkovnih postavk, ki se obdelujejo;
- trajanje ali stalnost dejavnosti obdelave podatkov in
- geografska razsežnost dejavnosti obdelave.

Primeri obsežne obdelave vključujejo:

- obdelavo podatkov o bolnikih s strani bolnišnice v okviru običajnega poslovanja;
- obdelavo potovalnih podatkov posameznikov, ki uporabljajo sistem javnega mestnega prevoza (npr. sledenje prek vozovnic);
- obdelavo podatkov o zemljepisnem položaju strank mednarodne verige hitre prehrane v realnem času za statistične namene s strani obdelovalca, specializiranega za te dejavnosti;
- obdelavo podatkov o strankah s strani zavarovalnice ali banke v okviru običajnega poslovanja;
- obdelavo osebnih podatkov za oglaševanje na podlagi vedenjskih vzorcev prek iskalnika in
- obdelavo podatkov (vsebine, prometa, lokacije) s strani ponudnikov telefonskih ali internetnih storitev.

Primeri neobsežne obdelave vključujejo:

- obdelavo podatkov o bolnikih s strani posameznega zdravnika in
- obdelavo osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški s strani posameznega odvetnika.

Več informacij je na voljo v oddelku 2.1.3 smernic.

4 Kaj pomeni pojem „redno in sistematično spremljanje“? (člen 37(1)(b))

Splošna uredba o varstvu podatkov ne opredeljuje pojma rednega in sistematičnega spremljanja posameznikov, na katere se nanašajo osebni podatki, vendar jasno vključuje vse oblike sledenja posameznikom in oblikovanja njihovega profila na internetu, tudi zaradi oglaševanja na podlagi vedenjskih vzorcev. Vendar pa pojem spremljanja ni omejen na spletno okolje.

Po razlagi delovne skupine iz člena 29 izraz „redno“ pomeni eno ali več od naslednjega:

- ki poteka ali nastopa v določenih intervalih in določenem obdobju;
- ki se izvaja večkrat ali se ponavlja ob določenem času;
- ki se izvaja stalno ali periodično.

Po razlagi delovne skupine iz člena 29 izraz „sistematično“ pomeni eno ali več od naslednjega:

- ki se izvaja v skladu s sistemom;
- ki je vnaprej določeno, organizirano ali metodično;
- ki poteka kot del splošnega načrta zbiranja podatkov;
- ki se izvaja kot del strategije.

Primeri: upravljanje telekomunikacijskega omrežja, zagotavljanje telekomunikacijskih storitev, ponovno ciljanje prek e-pošte, oblikovanje profilov in točkovanje za namene ocene tveganja (npr. zaradi kreditnega točkovanja, določitve zavarovalnih premij, preprečevanja goljufij, odkrivanja pranja denarja), sledenje geografskemu položaju, na primer z mobilnimi napravami, programi zvestobe, oglaševanje na podlagi vedenjskih vzorcev, spremljanje podatkov o dobrem počutju, telesni pripravljenosti in zdravju prek nosljivih naprav, sistem televizije zaprtega kroga, povezane naprave, npr. pametni števeci, pametni avtomobili, avtomatizacija doma itd.

Več informacij je na voljo v oddelku 2.1.4 smernic.

5 Ali lahko organizacije pooblaščen osebo za varstvo podatkov imenujejo skupaj? Če je odgovor pritrdilen, pod katerimi pogoji? (člen 37(2) in (3))

V skladu s Splošno uredbo o varstvu podatkov lahko povezana družba imenuje eno pooblaščen osebo za varstvo podatkov, če je ta oseba „lahko dostopna iz vsake enote“. Pojem dostopnosti se nanaša na naloge pooblaščen osebe za varstvo podatkov kot kontaktne točke za posameznike, na katere se nanašajo osebni podatki, nadzorni organ, pa tudi znotraj organizacije. Za zagotovitev dostopnosti pooblaščen osebe za varstvo podatkov, bodisi notranje ali zunanje, je treba poskrbeti, da bodo v skladu s Splošno uredbo o varstvu podatkov na voljo njeni kontaktni podatki. Pooblaščen oseba za varstvo podatkov mora biti sposobna učinkovito komunicirati s posamezniki, na katere se nanašajo osebni podatki, in sodelovati z zadevnimi nadzornimi organi. To pomeni, da mora ta komunikacija potekati v jeziku ali jezikih, ki jih uporabljajo zadevni nadzorni organi in posamezniki, na katere se nanašajo osebni podatki. Dostopnost pooblaščen osebe za varstvo podatkov (bodisi fizična v istih prostorih kot zaposleni, prek namenske telefonske linije ali drugih varnih komunikacijskih sredstev) je bistvena za zagotovitev, da bodo lahko posamezniki, na katere se nanašajo osebni podatki, stopili v stik z njo.

Več informacij je na voljo v oddelku 2.3 smernic.

6 Ali se lahko imenuje zunanja pooblaščen oseba za varstvo podatkov (člen 37(6))?

Da. V skladu s členom 37(6) je lahko pooblaščen oseba za varstvo podatkov član osebja upravljavca ali obdelovalca (notranja pooblaščen oseba za varstvo podatkov) ali pa „naloge opravlja na podlagi pogodbe o storitvah“. To pomeni, da je lahko pooblaščen oseba za varstvo podatkov zunanja in lahko svojo funkcijo izvaja na podlagi pogodbe o storitvah, ki jo sklene s posameznikom ali organizacijo.

Če je pooblaščen oseba za varstvo podatkov zunanja, zanjo veljajo vse zahteve iz členov 37 do 39. V smernicah je navedeno, da kadar funkcijo pooblaščen osebe za varstvo podatkov opravlja zunanji ponudnik storitev, lahko ekipa posameznikov, ki delajo za ta subjekt, kot taka učinkovito izvaja naloge pooblaščen osebe za varstvo podatkov v okviru odgovornosti pooblaščen glavne kontaktne osebe in „pristojne osebe“ za stranko. V tem primeru je bistveno, da vsak član zunanje organizacije, ki izvaja funkcije pooblaščen osebe za varstvo podatkov, izpolnjuje vse ustrezne zahteve iz Splošne uredbe o varstvu podatkov.

Zaradi pravne jasnosti in dobre organizacije je v smernicah priporočeno, da se v pogodbi o storitvah jasno razdelijo naloge v ekipi zunanje pooblaščen osebe za varstvo podatkov in da se za glavno kontaktno točko in „pristojno“ osebo za stranko določi en posameznik.

Več informacij je na voljo v oddelkih 2.3, 2.4 in 3.5 smernic.

7 Katere poklicne odlike bi morala imeti pooblaščenca oseba za varstvo podatkov (člen 37(5))?

Splošna uredba o varstvu podatkov določa, da se pooblaščenca oseba za varstvo podatkov „*imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog iz člena 39*“.

Raven potrebnega strokovnega znanja bi bilo treba določiti glede na dejanja obdelave podatkov, ki se izvajajo, in varstvo, ki je potrebno pri osebnih podatkih, ki se obdelujejo. Kadar je na primer dejavnost obdelave podatkov posebno zapletena ali se obdeluje velika količina občutljivih podatkov, bo pooblaščenca oseba za varstvo podatkov morda potrebovala višjo raven strokovnega znanja in podpore.

Potrebne spretnosti in strokovno znanje vključujejo:

- strokovno znanje o nacionalnih in evropskih zakonih in praksah na področju varstva podatkov ter poglobljeno razumevanje Splošne uredbe o varstvu podatkov;
- razumevanje dejanj obdelave, ki se izvajajo;
- razumevanje informacijskih tehnologij in varstva podatkov;
- poznavanje poslovnega sektorja in organizacije ter
- sposobnost spodbujanja kulture varstva podatkov v organizaciji.

Več informacij je na voljo v oddelku 2.4 smernic.

Položaj pooblaščenca osebe za varstvo podatkov (člen 38)

8 Katera sredstva je treba zagotoviti pooblaščenca osebi za varstvo podatkov, da lahko ta izvaja svoje naloge?

Člen 38(2) Splošne uredbe o varstvu podatkov določa, da organizacija pooblaščenca osebi za varstvo podatkov „*[zagotovi] sredstva, potrebna za opravljanje [njenih] nalog, in dostop do osebnih podatkov in dejanj obdelave, ter ohranjanje njenega strokovnega znanja*“.

Glede na naravo dejanj in dejavnosti obdelave ter velikost organizacije bi bilo treba pooblaščenca osebi za varstvo podatkov zagotoviti naslednja sredstva:

- aktivno podporo funkcije pooblaščenca osebe za varstvo podatkov s strani višjega vodstva;
- zadostni čas, v katerem lahko pooblaščenca oseba izpolni svoje dolžnosti;
- zadostno podporo v smislu finančnih sredstev, infrastrukture (prostori, objekti, oprema) in po potrebi osebja;
- uradno sporočilo vsem članom osebja o imenovanju pooblaščenca osebe za varstvo podatkov;
- dostop do drugih služb v organizaciji, da lahko pooblaščenca osebe za varstvo podatkov od teh služb prejmejo potrebno podporo, prispevek in informacije, ter
- stalno usposabljanje.

Več informacij je na voljo v oddelku 3.2 smernic.

9 Kateri zaščitni ukrepi pooblašчени osebi za varstvo podatkov omogočajo neodvisno izvajanje nalog (člen 38(3))?

Neodvisno delovanje pooblaščenih oseb za varstvo podatkov se omogoča z več zaščitnimi ukrepi iz uvodne izjave 97:

- pooblaščen oseba za varstvo podatkov pri opravljanju svojih nalog ne prejema nobenih navodil od upravljavcev ali obdelovalcev;
- upravljavec pooblaščenih oseb za varstvo podatkov ne sme razrešiti zaradi opravljanja njenih nalog ter
- preprečujejo se nasprotja interesov zaradi morebitnih drugih nalog in dolžnosti.

Več informacij je na voljo v oddelkih 3.3 do 3.5 smernic.

10 Katere so „druge naloge in dolžnosti“ pooblaščenih oseb za varstvo podatkov, ki lahko povzročijo nasprotja interesov (člen 38(6))?

Pooblaščen oseba za varstvo podatkov v organizaciji ne sme zavzemati položaja, ki ji omogoča določanje namenov in sredstev obdelave osebnih podatkov. Zaradi posebne organizacijske strukture vsake organizacije je treba to obravnavati za vsak primer posebej.

Splošno gledano lahko nasprotujoči si položaji vključujejo položaje višjega vodstva (kot so izvršni direktor, operativni direktor, finančni direktor, vodja zdravstvene službe, vodja oddelka za trženje, vodja službe za človeške vire ali vodja oddelkov za informacijsko tehnologijo) in tudi druge vloge na nižji ravni organizacijske strukture, če taki položaji ali vloge zajemajo določanje namenov in sredstev obdelave.

Več informacij je na voljo v oddelku 3.5 smernic.

Naloge pooblaščenih oseb za varstvo podatkov (člen 39)

11 Kaj zajema pojem „spremljanje skladnosti“ s Splošno uredbo o varstvu podatkov (člen 39(1)(b))?

Pooblaščen osebe za varstvo podatkov lahko kot del teh dolžnosti spremljanja skladnosti zlasti:

- zbirajo informacije za opredelitev dejavnosti obdelave,
- analizirajo in preverjajo skladnost dejavnosti obdelave ter
- obveščajo upravljavca ali obdelovalca, mu svetujejo in zanj izdajajo priporočila.

Več informacij je na voljo v oddelku 4.1 smernic.

12 Ali je pooblaščen osebno odgovorna za neskladnost s Splošno uredbo o varstvu podatkov?

Ne. Pooblaščen osebno odgovorne za neskladnost s Splošno uredbo o varstvu podatkov. V Splošni uredbi o varstvu podatkov je jasno navedeno, da je upravljavec ali obdelovalec tisti, ki mora zagotoviti in biti zmožen dokazati, da obdelava poteka v skladu s to uredbo (člen 24(1)). Zagotavljanje skladnosti z določbami o varstvu podatkov je odgovornost upravljavca ali obdelovalca.

13 Kakšno vlogo ima pooblaščen osebno odgovorna za oceno učinka v zvezi z varstvom podatkov (člen 37(1)(c) in evidenci dejavnosti obdelave (člen 30)?

Glede ocene učinka v zvezi z varstvom podatkov bi moral upravljavec ali obdelovalec pooblaščen osebno odgovorna za varstvo podatkov med drugim prositi za mnenje o naslednjih vprašanjih:

- ali naj izvede oceno učinka v zvezi z varstvom podatkov ali ne;
- katero metodologijo naj uporabi pri izvajanju ocene učinka v zvezi z varstvom podatkov;
- ali naj oceno učinka v zvezi z varstvom podatkov izvede interno ali naj jo odda v zunanje izvajanje;
- katere zaščitne ukrepe (vključno s tehničnimi in organizacijskimi ukrepi) naj uporabi za zmanjševanje morebitnih tveganj za pravice in interese posameznikov, na katere se nanašajo osebni podatki, in
- ali je bila ocena učinka v zvezi z varstvom podatkov pravilno izvedena in ali so njene ugotovitve (ali naj se obdelava nadaljuje ali ne in kateri zaščitni ukrepi naj se uporabijo) v skladu s Splošno uredbo o varstvu podatkov.

Več informacij je na voljo v oddelku 4.2 smernic.

V zvezi z evidenco dejavnosti obdelave mora evidenco dejanj obdelave voditi upravljavec ali obdelovalec in ne pooblaščen osebno odgovorna za varstvo podatkov. Vendar upravljavcu ali obdelovalcu nič ne preprečuje, da pooblaščen osebno odgovorna za varstvo podatkov dodeli nalogo vodenja evidence dejanj obdelave v okviru odgovornosti upravljavca. Tako evidenco bi bilo treba obravnavati kot eno od orodij, ki pooblaščen osebno odgovorna za varstvo podatkov omogočajo izvajanje nalog spremljanja skladnosti ter obveščanja upravljavca ali obdelovalca in svetovanja upravljavcu ali obdelovalcu.

Več informacij je na voljo v oddelku 4.4 smernic.