Smernice št. 4/2019 o členu 25

Vgrajeno in privzeto varstvo podatkov

Različica 2.0

Sprejete 20. oktobra 2020

Zgodovina različic

Različica 1.0	13. november 2019	Sprejetje Smernic za javno posvetovanje
Različica 2.0	20. oktober 2020	Sprejetje smernic s strani Evropskega odbora za varstvo podatkov po javnem posvetovanju

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018,

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE

Povzetek

V čedalje bolj digitaliziranem svetu ima zavezanost zahtevam vgrajenega in privzetega varstva podatkov odločilno vlogo pri spodbujanju zasebnosti in varstva podatkov v družbi. Zato je bistveno, da upravljavci resno vzamejo to odgovornost in pri oblikovanju dejanj obdelave izvajajo obveznosti iz Splošne uredbe o varstvu podatkov.

Te smernice vsebujejo splošne smernice o obveznosti vgrajenega in privzetega varstva podatkov iz člena 25 Splošne uredbe o varstvu podatkov. Vgrajeno in privzeto varstvo podatkov je obveznost za vse upravljavce ne glede na velikost in zapletenost obdelave. Da bi upravljavec lahko izvajal zahteve vgrajenega in privzetega varstva podatkov, je bistveno, da razume načela varstva podatkov ter pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

Temeljna obveznost je izvajanje *ustreznih* ukrepov in potrebnih zaščitnih ukrepov, ki zagotavljajo *učinkovito izvajanje načel varstva podatkov* ter posledično *vgrajenih in privzetih pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki*. Člen 25 določa elemente vgrajenega in privzetega varstva, ki jih je treba upoštevati. Te smernice podrobneje opredeljujejo te elemente.

Člen 25(1) določa, da morajo upravljavci vgrajeno in privzeto varstvo podatkov upoštevati že pri načrtovanju novega dejanja obdelave. Upravljavci izvajajo vgrajeno in privzeto varstvo podatkov *pred* obdelavo in tudi *neprekinjeno* med obdelavo, tako da redno pregledujejo učinkovitost izbranih ukrepov in zaščitnih ukrepov. Vgrajeno in privzeto varstvo podatkov se uporablja tudi za obstoječe sisteme, ki obdelujejo osebne podatke.

Smernice vsebujejo tudi navodila, kako učinkovito izvajati načela varstva podatkov iz člena 5, saj so v njih navedeni ključni vgrajeni in privzeti elementi ter praktični primeri za ponazoritev. Upravljavec mora preučiti ustreznost predlaganih ukrepov v okviru posamezne zadevne obdelave.

Evropski odbor za varstvo podatkov zagotavlja priporočila, kako lahko upravljavci, obdelovalci in proizvajalci sodelujejo, da bi dosegli vgrajeno in privzeto varstvo podatkov. Upravljavce v panogi, obdelovalce in proizvajalce spodbuja, naj pri trženju svojih proizvodov upravljavcem in posameznikom, na katere se nanašajo osebni podatki, uporabljajo vgrajeno in privzeto varstvo podatkov kot sredstvo za doseganje konkurenčne prednosti. Poleg tega vse upravljavce spodbuja k uporabi potrdil in kodeksov ravnanja.

1 PODROČJE UPORABE

1. Smernice se osredotočajo na izvajanje vgrajenega in privzetega varstva podatkov s strani upravljavcev na podlagi obveznosti iz člena 25 Splošne uredbe o varstvu podatkov.[1] Te smernice lahko koristijo tudi drugim izvajalcem, kot so obdelovalci podatkov ter proizvajalci izdelkov, storitev in aplikacij, ki v členu 25 niso neposredno obravnavani, ko ustvarjajo izdelke in storitve, skladne s Splošno uredbo o varstvu podatkov, ki omogočajo upravljavcem, da izpolnijo obveznosti glede varstva podatkov.[2] V uvodni izjavi 78 Splošne uredbe o varstvu podatkov je navedeno, da bi morali vgrajeno in privzeto varstvo podatkov upoštevati tudi pri javnih razpisih. Čeprav morajo vgrajeno in privzeto varstvo podatkov v svoje dejavnosti obdelave vključiti vsi upravljavci, ta določba spodbuja sprejetje načel varstva podatkov, pri katerih bi morale javne uprave dajati vzgled. Upravljavec podatkov je odgovoren za izpolnjevanje obveznosti vgrajenega in privzetega varstva podatkov pri obdelavi, ki jo izvajajo njegovi obdelovalci in podobdelovalci, zato bi moral to upoštevati pri sklepanju pogodb s temi strankami.

2. Zahteva iz člena 25 določa, da morajo upravljavci zagotoviti, da je varstvo podatkov vgrajeno v obdelavo osebnih podatkov in privzeto, kar velja za celoten življenjski cikel obdelave. Zahteva vgrajenega in privzetega varstva podatkov velja tudi za sisteme obdelave, ki so obstajali že pred začetkom veljavnosti Splošne uredbe o varstvu podatkov. Upravljavci morajo zagotoviti, da se obdelava dosledno posodablja v skladu s Splošno uredbo o varstvu podatkov. Za več informacij o tem, kako obstoječi sistem vzdrževati v skladu z vgrajenim in privzetim varstvom podatkov, glej podpoglavje 2.1.4 teh smernic. Bistvo določbe je zagotoviti *ustrezno* in *učinkovito* varstvo podatkov, ki je *vgrajeno* in *privzeto*, kar pomeni, da bi morali biti upravljavci zmožni dokazati, da imajo pri obdelavi podatkov ustrezne ukrepe in zaščitne ukrepe, ki zagotavljajo, da so načela varstva podatkov ter pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, učinkoviti.

3. Poglavje 2 Smernic se osredotoča na razlago zahtev iz člena 25 in preučuje pravne obveznosti določbe. Poglavje 3 obravnava primere, kako uporabiti vgrajeno in privzeto varstvo podatkov v okviru posebnih načel varstva podatkov.

4. V poglavju 4 Smernic je obravnavana možnost uvedbe mehanizma potrjevanja za dokazovanje skladnosti s členom 25, v poglavju 5 pa, kako lahko nadzorni organi izvršujejo ta člen. Na koncu Smernice vsebujejo nadaljnja priporočila deležnikom za uspešno izvajanje vgrajenega in privzetega varstva podatkov. Evropski odbor za varstvo podatkov priznava izzive, s katerimi se mala in srednja podjetja (MSP) srečujejo pri polnem izpolnjevanju obveznosti vgrajenega in privzetega varstva podatkov, zato v poglavju 6 podaja dodatna priporočila posebej zanje.

[1] Razlage iz teh smernic se nanašajo tudi na člen 20 Direktive (EU) 2016/680 in člen 27 Uredbe 2018/1725.

[2] V uvodni izjavi 78 je ta potreba jasno navedena: „*Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi osebnih podatkov ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, bi bilo treba proizvajalce produktov, storitev in aplikacij spodbujati, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju [,]najnovejšega tehnološkega razvoja[‘], zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov*“.

2 ANALIZA ČLENA 25(1) IN (2) – VGRAJENO IN PRIVZETO VARSTVO PODATKOV

5. Namen tega poglavja je preučiti in zagotoviti smernice o zahtevah glede vgrajenega varstva podatkov iz člena 25(1) in privzetega varstva podatkov iz člena 25(2)Splošne uredbe o varstvu podatkov. Vgrajeno varstvo podatkov in privzeto varstvo podatkov sta dopolnjujoča se koncepta, ki se medsebojno krepita. Posamezniki, na katere se nanašajo osebni podatki, bodo od privzetega varstva podatkov imeli več koristi, če se hkrati izvaja vgrajeno varstvo podatkov, in obratno.

6. Vgrajeno in privzeto varstvo podatkov je zahteva za vse upravljavce in vključuje tako mala podjetja kot tudi večnacionalne gospodarske družbe. Zato je lahko zapletenost izvajanja vgrajenega in privzetega varstva podatkov odvisna od posameznega dejanja obdelave. Ne glede na velikost pa se lahko pozitivne koristi za upravljavca in posameznika, na katerega se nanašajo osebni podatki, v vseh primerih dosežejo z izvajanjem vgrajenega in privzetega varstva podatkov.

2.1 Člen 25(1): Vgrajeno varstvo podatkov

2.1.1 Obveznost upravljavca, da pri obdelavi izvaja ustrezne tehnične in organizacijske ukrepe ter potrebne zaščitne ukrepe.

7. V skladu s členom 25(1) mora upravljavec izvajati *ustrezne* tehnične in organizacijske *ukrepe*, namenjene izvajanju načel varstva podatkov in vključitvi *potrebnih zaščitnih ukrepov* v obdelavo, da se izpolnijo zahteve ter zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Namen ustreznih ukrepov in potrebnih zaščitnih ukrepov je enak, to je varstvo pravic posameznikov, na katere se nanašajo osebni podatki, in zagotovitev, da je varstvo osebnih podatkov vgrajeno v obdelavo.

8. *Tehnične in organizacijske ukrepe* ter potrebne *zaščitne ukrepe* je mogoče razumeti široko kot metodo ali način, ki jo upravljavec lahko uporabi pri obdelavi. *Ustreznost* pomeni, da bi morali biti ukrepi in potrebni zaščitni ukrepi primerni za doseganje predvidenega namena, tj. da morajo načela varstva podatkov izvajati *učinkovito*.[3] Zahteva po ustreznosti je tako tesno povezana z zahtevo po učinkovitosti.

9. Tehnični ali organizacijski ukrep in zaščitni ukrep lahko zajemata kar koli, od uporabe naprednih tehničnih rešitev do osnovnega usposabljanja osebja. Primeri, ki so lahko ustrezni, odvisno od okoliščin in tveganj, povezanih z zadevno obdelavo, vključujejo psevdonimizacijo osebnih podatkov,[4] shranjevanje osebnih podatkov, ki so na voljo v strukturirani, običajno strojno berljivi obliki, omogočanje posameznikom, na katere se nanašajo osebni podatki, da posredujejo pri obdelavi, zagotavljanje informacij o shranjevanju osebnih podatkov, posedovanje sistemov za odkrivanje zlonamerne programske opreme, usposabljanje zaposlenih o osnovni „kibernetski higieni“, vzpostavitev sistemov za upravljanje zasebnosti in informacijske varnosti, ki obdelovalce pogodbeno zavezuje k izvajanju posebnih praks najmanjšega obsega podatkov, itd.

10. Pri določanju ustreznih ukrepov so lahko koristni standardi, dobra praksa ter kodeksi ravnanja, ki jih priznavajo združenja in drugi organi, ki zastopajo kategorije upravljavcev. Upravljavec mora preveriti ustreznost ukrepov za posamezno zadevno obdelavo.

[3] „Učinkovitost“ je obravnavana v nadaljevanju, v podpoglavju 2.1.2.
[4] Opredeljeno v členu 4(5) Splošne uredbe o varstvu podatkov.

2.1.2 Oblikovanje ukrepov za učinkovito izvajanje načel varstva podatkov ter varovanje pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki

11. *Načela varstva podatkov* so navedena v členu 5 (v nadaljevanju: načela), *pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki*, pa so temeljne pravice in svoboščine fizičnih oseb, zlasti pa njihova pravica do varstva osebnih podatkov, katere varstvo je v členu 1(2) navedeno kot cilj Splošne uredbe o varstvu podatkov (v nadaljevanju: pravice).[5] Njihova natančna ubeseditev je na voljo v Listini EU o temeljnih pravicah. Bistveno je, da upravljavec razume pomen *načel* in *pravic* kot podlago za varstvo, ki ga zagotavlja Splošna uredba o varstvu podatkov, zlasti z obveznostjo vgrajenega in privzetega varstva podatkov.

12. Pri izvajanju ustreznih tehničnih in organizacijskih ukrepov je pomembno, da so ukrepi in zaščitni ukrepi *oblikovani* ob upoštevanju učinkovitega izvajanja vsakega od zgoraj navedenih načel in posledičnega varstva pravic.

Obravnavanje učinkovitosti

13. Učinkovitost je v središču pojma vgrajenega varstva podatkov. Zahteva po učinkovitem izvajanju načel pomeni, da morajo upravljavci izvajati potrebne ukrepe in zaščitne ukrepe za zaščito teh načel, da se zavarujejo pravice posameznikov, na katere se nanašajo osebni podatki. Z vsakim izvedenim ukrepom je treba zagotoviti rezultate za obdelavo, ki jih predvideva upravljavec. Ta ugotovitev ima dve posledici.

14. Prvič, to pomeni, da člen 25 ne določa izvajanja posebnih tehničnih in organizacijskih ukrepov, ampak da morajo biti izbrani ukrepi in zaščitni ukrepi specifični za izvajanje načel varstva podatkov pri posamezni zadevni obdelavi. Pri tem bi morali biti ukrepi in zaščitni ukrepi oblikovani tako, da bi bili zanesljivi, upravljavec pa bi moral biti zmožen izvajati nadaljnje ukrepe v zvezi z morebitnim povečanjem tveganja.[6] Ali so ukrepi učinkoviti ali ne, je torej odvisno od okoliščin zadevne obdelave in ocene nekaterih elementov, ki bi jih bilo treba upoštevati pri določitvi sredstev obdelave. Zgoraj navedeni elementi so obravnavani v nadaljevanju v podpoglavju 2.1.3.

15. Drugič, upravljavci bi morali biti sposobni dokazati, da se načela upoštevajo.

16. Z izvedenimi ukrepi in zaščitnimi ukrepi je treba doseči želeni učinek v smislu varstva podatkov, upravljavec pa bi moral imeti dokumentacijo o izvedenih tehničnih in organizacijskih ukrepih.[7] Upravljavec lahko učinkovitost dokaže tako, da določi ustrezne ključne kazalnike uspešnosti. Ključni kazalniki uspešnosti so izmerljiva vrednost, ki jo izbere upravljavec in s katero dokaže, kako učinkovito dosega svoj cilj varstva podatkov. Ključni kazalniki uspešnosti so lahko *količinski*, kot so delež lažno pozitivnih ali lažno negativnih rezultatov, manjše število pritožb, krajši odzivni čas pri uresničevanju pravic posameznikov, na katere se nanašajo osebni podatki, ali *kakovostni*, kot so ocenjevanje uspešnosti, razvrstitvene lestvice ali strokovne ocene. Namesto ključnih kazalnikov uspešnosti lahko

[5] Glej uvodno izjavo 4 Splošne uredbe o varstvu podatkov.

[6] „Temeljna načela, ki se uporabljajo za upravljavce (tj. zakonitost, najmanjši obseg podatkov, omejitev namena, preglednost, celovitost, točnost podatkov), morajo ostati nespremenjena ne glede na obdelavo in tveganja za posameznike, na katere se nanašajo osebni podatki. Vendar pa glede na to, da sta bila narava in obseg take obdelave vedno sestavni del uporabe teh načel, ju je mogoče po svojstvu nadgraditi.“ Delovna skupina iz člena 29. „Izjava o vlogi pristopa na podlagi tveganja v pravnih okvirih v zvezi z varstvom podatkov“. WP 218, 30. maj 2014, str. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Glej uvodni izjavi 74 in 78.

upravljavci učinkovito izvajanje načel dokažejo tako, da utemeljijo svojo oceno učinkovitosti izbranih ukrepov in zaščitnih ukrepov.

2.1.3 Elementi, ki jih je treba upoštevati

17. V členu 25(1) so navedeni elementi, ki jih mora upravljavec upoštevati pri določitvi ukrepov posebnega dejanja obdelave. V nadaljevanju so navedene smernice, kako te elemente uporabljati v postopku oblikovanja, ki vključuje oblikovanje privzetih nastavitev. Vsi ti elementi pripomorejo k odločitvi, ali je ukrep ustrezen za učinkovito izvajanje načel. Zato niso cilj sami po sebi, ampak so dejavniki, ki jih je treba za dosego cilja obravnavati skupaj.

2.1.3.1 „Najnovejši tehnološki razvoj“

18. Pojem „najnovejši tehnološki razvoj“ je prisoten na različnih področjih pravnega reda EU, na primer pri varstvu okolja in varnosti izdelkov. V Splošni uredbi o varstvu podatkov sklicevanje na „najnovejši tehnološki razvoj”[8] ni navedeno le v členu 32 glede varnostnih ukrepov,[9][10] ampak tudi v členu 25, s čimer se to referenčno merilo nanaša na vse tehnične in organizacijske ukrepe, vključene v obdelavo.

19. V okviru člena 25 sklicevanje na „najnovejši tehnološki razvoj“ nalaga obveznost upravljavcem, da pri določitvi ustreznih tehničnih in organizacijskih ukrepov **upoštevajo sedanji napredek v tehnologiji**, ki je na voljo na trgu. Ta zahteva pomeni, da morajo upravljavci poznati tehnološki napredek in stalno slediti njegovemu razvoju, poznati tveganja ali priložnosti tehnologije za varnost dejanja obdelave ter načine, kako izvajati in posodabljati ukrepe in zaščitne ukrepe, ki *zagotavljajo učinkovito izvajanje* načel in pravic posameznikov, na katere se nanašajo osebni podatki, ob upoštevanju razvijajočega se tehnološkega okolja.

20. „Najnovejši tehnološki razvoj“ je dinamičen pojem, ki ga ni mogoče statično opredeliti v posamezni časovni točki, ampak ga je treba *nenehno* ocenjevati v okviru tehnološkega napredka. Upravljavec lahko glede na tehnološki napredek ugotovi, da ukrep, ki je včasih zagotavljal ustrezno stopnjo varstva, ni več učinkovit. Opustitev spremljanja tehnoloških sprememb lahko torej povzroči neskladnost s členom 25.

21. Merilo „najnovejšega tehnološkega razvoja“ se ne nanaša le na tehnološke, ampak tudi na organizacijske ukrepe. Pomanjkanje ustreznih organizacijskih ukrepov lahko zmanjša ali popolnoma oslabi učinkovitost izbrane tehnologije. Primeri organizacijskih ukrepov so lahko sprejetje notranjih politik, najnovejše usposabljanje o tehnologiji, varnosti in varstvu podatkov ter politike upravljanja in vodenja varnosti IT.

22. Obstoječi in priznani okviri, standardi, potrdila, kodeksi ravnanja itd. na različnih področjih lahko vplivajo na navedbo trenutnega „najnovejšega tehnološkega razvoja“ na danem področju uporabe. Kadar so taki standardi sprejeti in zagotavljajo visoko raven varstva posameznika, na katerega se

[8] Glej sklep nemškega zveznega ustavnega sodišča v zadevi *Kalkar* iz leta 1978: https://germanlawarchive.iuscomp.org/?p=67, ki je lahko podlaga za metodologijo objektivne opredelitve pojma. Na tej podlagi bi bila stopnja „najnovejšega tehnološkega razvoja“ opredeljena med tehnološko ravnjo „obstoječega znanstvenega znanja in raziskav“ in bolj uveljavljenimi „splošno sprejetimi tehnološkimi pravili“. „Najnovejši tehnološki razvoj“ je torej mogoče opredeliti kot tehnološko stopnjo storitve, tehnologije ali izdelka, ki obstaja na trgu in je najučinkovitejša za doseganje opredeljenih ciljev.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/.

nanašajo osebni podatki, v skladu s pravnimi zahtevami ali jih presegajo, bi jih morali upravljavci upoštevati pri oblikovanju in izvajanju ukrepov za varstvo podatkov.

2.1.3.2 „Stroški izvajanja“

23. Upravljavec lahko pri izbiri in uporabi ustreznih tehničnih in organizacijskih ukrepov ter potrebnih zaščitnih ukrepov, s katerimi se učinkovito izvajajo načela za zaščito pravic posameznikov, na katere se nanašajo osebni podatki, upošteva stroške izvajanja. Stroški se nanašajo na vire na splošno, vključno s časom in človeškimi viri.

24. Stroškovni element od upravljavca ne zahteva, da porabi nesorazmerno količino virov, kadar so na voljo alternativni ukrepi, za katere je potrebnih manj sredstev, vendar so učinkoviti. Vendar so stroški izvajanja dejavnik, ki ga je treba upoštevati pri izvajanju vgrajenega varstva podatkov, in ne razlog za neizvajanje.

25. Z izbranimi ukrepi se zato zagotovi, da se v okviru dejavnosti obdelave, ki jo predvideva upravljavec, osebni podatki ne obdelujejo v nasprotju z načeli, ne glede na stroške. Upravljavci bi morali biti zmožni upravljati skupne stroške, da bi lahko učinkovito izvajali vsa načela in tako zaščitili pravice.

2.1.3.3 „Narava, obseg, okoliščine in namen obdelave“

26. Upravljavci morajo pri določanju potrebnih ukrepov upoštevati naravo, obseg, okoliščine in namen obdelave.

27. Te dejavnike je treba razlagati v skladu z njihovo vlogo v drugih določbah Splošne uredbe o varstvu podatkov, kot so členi 24, 32 in 35, cilj tega pa mora biti vgradnja načel varstva podatkov v obdelavo.

28. Na kratko, pojem **narava** je mogoče razumeti kot notranje[11] značilnosti obdelave. **Obseg** se nanaša na obseg in vrsto obdelave. **Okoliščine** se nanašajo na okoliščine obdelave, ki lahko vplivajo na pričakovanja posameznika, na katerega se nanašajo osebni podatki, **namen** pa se nanaša na cilje obdelave.

2.1.3.4 „Tveganja za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti“

29. Zaradi opredelitve ustreznih tehničnih in organizacijskih ukrepov za varstvo posameznikov in njihovih osebnih podatkov ter izpolnitve zahteve Splošne uredbe o varstvu podatkov je v več njenih določbah, in sicer v členih 24, 25, 32 in 35, uporabljen skladen pristop na podlagi tveganja. Sredstva, ki jih je treba varovati (posamezniki prek varovanja njihovih osebnih podatkov), tveganja, pred katerimi jih je treba varovati (za pravice posameznikov), in pogoji, ki jih je treba upoštevati (narava, obseg, okoliščine in namen obdelave), so vedno enaki.

30. Pri izvajanju analize tveganja za skladnost s členom 25 mora upravljavec opredeliti tveganja za pravice posameznikov, na katere se nanašajo osebni podatki, ki jih predstavlja kršitev načel, ter določiti njihovo verjetnost in resnost, da lahko izvede ukrepe za učinkovito ublažitev opredeljenih tveganj. Pri ocenjevanju tveganja je bistveno sistematično in temeljito vrednotenje obdelave. Upravljavec na primer oceni posebna tveganja, povezana z odsotnostjo prostovoljne privolitve, kar pomeni kršitev načela zakonitosti, pri obdelavi osebnih podatkov otrok in mladih, starih manj kot 18 let, kot ranljive

[11] Primeri so posebne kategorije osebnih podatkov, samodejno sprejemanje odločitev, izkrivljena razmerja moči, nepredvidljiva obdelava, težave posameznika, na katerega se nanašajo osebni podatki, pri uveljavljanju pravic itd.

skupine, kadar ni druge pravne podlage, ter izvede ustrezne ukrepe za obravnavanje in učinkovito ublažitev opredeljenih tveganj, povezanih s to skupino posameznikov, na katere se nanašajo osebni podatki.

31. „Smernice Evropskega odbora za varstvo podatkov o oceni učinka v zvezi z varstvom podatkov (DPIA)“,[12] ki se osredotočajo na določanje, ali obstaja verjetnost, da bo dejanje obdelave povzročilo visoko tveganje za posameznika, na katerega se nanašajo osebni podatki, ali ne, zagotavljajo tudi smernice, kako oceniti tveganja glede varstva podatkov in kako to oceno izvesti. Te smernice so lahko koristne tudi za oceno tveganja iz vseh zgoraj navedenih členov, vključno s členom 25.

32. Pristop na podlagi tveganja ne izključuje uporabe izhodišč, dobre prakse in standardov. Za upravljavce so to lahko koristna orodja za spopadanje s podobnimi tveganji v podobnih situacijah (narava, obseg, okoliščine in namen obdelave). Vendar ostaja obveznost iz člena 25 (in tudi členov 24, 32 in 35(7)(c)), da je treba upoštevati *„tveganja za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti*“. Zato morajo upravljavci, čeprav imajo podporo takih orodij, pri zadevni dejavnosti obdelave vedno opraviti oceno tveganj glede varstva podatkov za vsak primer posebej ter preveriti učinkovitost predlaganih ustreznih ukrepov in zaščitnih ukrepov. Nato se lahko dodatno zahteva ocena učinka glede varstva podatkov ali posodobitev obstoječe ocene učinka glede varstva podatkov.

2.1.4 Časovni vidik

2.1.4.1 V času določitve sredstev obdelave

33. Vgrajeno varstvo podatkov se izvede *„v času določitve sredstev obdelave*“.

34. „*Sredstva obdelave*“ vključujejo od splošnih do podrobnih elementov oblikovanja obdelave, vključno z arhitekturo, postopki, protokoli, postavitvijo in videzom.

35. „*Čas določitve sredstev obdelave*“ se nanaša na obdobje, v katerem upravljavec odloča, kako bo obdelava izvedena, ter način obdelave in mehanizme, ki se bodo uporabili za tako obdelavo. Upravljavec mora med sprejemanjem takih odločitev oceniti ustrezne ukrepe in zaščitne ukrepe za učinkovito izvajanje načel in pravic posameznikov, na katere se nanašajo osebni podatki, pri obdelavi, ter upoštevati elemente, kot so najnovejši tehnološki razvoj, stroški izvajanja, narava, obseg, okoliščine, namen in tveganja. To vključuje čas nabave in vpeljave programske opreme, strojne opreme in storitev za obdelavo podatkov.

36. Zgodnje upoštevanje vgrajenega in privzetega varstva podatkov je ključno za uspešno izvajanje načel in varstvo pravic posameznikov, na katere se nanašajo osebni podatki. Poleg tega bi bilo z vidika stroškov in koristi v interesu upravljavcev tudi, da vgrajeno in privzeto varstvo podatkov upoštevajo raje prej kot pozneje, saj bi lahko bilo problematično in drago pozneje spreminjati že sestavljene načrte ter že oblikovana dejanja obdelave.

2.1.4.2 V času same obdelave (ohranitev in pregled zahtev glede varstva podatkov)

37. Ko se obdelava začne, mora upravljavec še naprej ohranjati vgrajeno in privzeto varstvo podatkov, tj. nadalje učinkovito izvajati načela za zaščito pravic, upoštevati najnovejši tehnološki razvoj, vnovič oceniti stopnjo tveganja itd. Narava, obseg in okvir dejanj obdelave ter tveganje se lahko med obdelavo

[12] Delovna skupina iz člena 29. „Smernice o oceni učinka v zvezi z varstvom podatkov (DPIA) in določanjem, ali ‚obstaja verjetnost, da bo dejanje obdelave povzročilo visoko tveganje‘ za namene Uredbe 2016/679“. WP 248 rev.01, 4. oktober 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – ki jih je potrdil Evropski odbor za varstvo podatkov.

spremenijo, kar pomeni, da mora upravljavec svoja dejanja obdelave vnovič oceniti z rednimi pregledi in ocenami učinkovitosti izbranih ukrepov in zaščitnih ukrepov.

38. Obveznost ohranjanja, pregleda in po potrebi posodobitve dejanja obdelave se uporablja tudi za obstoječe sisteme. To pomeni, da je treba obstoječe sisteme, oblikovane pred začetkom veljavnosti Splošne uredbe o varstvu podatkov, pregledati in vzdrževati, da se zagotovi izvajanje ukrepov in zaščitnih ukrepov, s katerimi se učinkovito izvajajo načela in pravice posameznikov, na katere se nanašajo osebni podatki, kot je določeno v teh smernicah.

39. Ta obveznost se nanaša tudi na vsako obdelavo, ki jo izvedejo obdelovalci podatkov. Upravljavci bi morali dejanja obdelovalcev redno pregledovati in ocenjevati za zagotovitev, da omogočajo nenehno skladnost z načeli ter da glede tega upravljavcu podatkov omogočajo izpolnjevanje njegovih obveznosti.

2.2 Člen 25(2): Privzeto varstvo podatkov

2.2.1 Privzeto se obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave

40. „Privzeto“, kot je splošno opredeljeno v računalništvu, se nanaša na vnaprej obstoječo ali izbrano vrednost nastavitve, ki jo je mogoče konfigurirati in se dodeli programski aplikaciji, računalniškemu programu ali napravi. Take nastavitve se imenujejo tudi „prednastavitve“ ali „tovarniške prednastavitve“, zlasti za elektronske naprave.

41. Posledično se „privzeto“ pri obdelavi osebnih podatkov nanaša na sprejemanje odločitev o konfiguraciji vrednosti ali možnostih obdelave, ki so določene ali predpisane v sistemu obdelave, kot so programska aplikacija, storitev ali naprava, ali postopek ročne obdelave, ki vpliva na količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost.

42. Upravljavec bi moral izbrati in biti odgovoren za izvajanje privzetih nastavitev in možnosti obdelave tako, da se privzeto izvaja le obdelava, ki je nujna za doseganje posameznega zakonitega namena. Tukaj bi se morali upravljavci zanašati na svojo oceno potrebnosti obdelave glede na pravno podlago iz člena 6(1). To pomeni, da privzeto ne smejo zbirati več podatkov, kot je potrebno, zbranih podatkov ne smejo obdelati bolj, kot je potrebno za njihove namene, in podatkov ne smejo hraniti dlje, kot je potrebno. Osnovna zahteva je, da mora biti varstvo podatkov privzeto vključeno v obdelavo.

43. Upravljavec mora vnaprej določiti, za katere določene, izrecne in zakonite namene se osebni podatki zbirajo in obdelujejo.[13] Ukrepi morajo biti samodejno ustrezni za zagotavljanje, da se obdelajo samo osebni podatki, potrebni za vsak poseben namen obdelave. Smernice Evropskega nadzornika za varstvo podatkov za ocenjevanje potrebnosti in sorazmernosti ukrepov, ki omejujejo pravico do

[13] Člen 5(1)(b), (c), (d) in (e) Splošne uredbe o varstvu podatkov.

varstva osebnih podatkov, so lahko koristne tudi za odločanje, katere podatke je treba obdelati za doseganje posebnega namena.[14, 15, 16]

44. Če upravljavec uporablja programsko opremo tretje osebe ali serijsko programsko opremo, mora izvesti oceno tveganja za proizvod in zagotoviti, da so funkcije, ki nimajo pravne podlage ali niso združljive s predvidenimi nameni obdelave, izklopljene.

45. Enake ugotovitve se nanašajo na organizacijske ukrepe, ki podpirajo dejanja obdelave. Oblikovani bi morali biti tako, da se na začetku z njimi obdela le minimalna količina osebnih podatkov, potrebnih za posebne obdelave. To je treba še posebej upoštevati pri dodeljevanju dostopa osebju z različnimi vlogami in različnimi potrebami glede dostopa.

46. Ustrezne „tehnične in organizacijske ukrepe“ v okviru privzetega varstva podatkov torej razumemo enako, kot je bilo obravnavano v podpoglavju 2.1.1 zgoraj, vendar se to še posebej nanaša na izvajanje načela najmanjšega obsega podatkov.

47. Zgoraj navedena obveznost, da se obdelajo samo osebni podatki, potrebni za vsak poseben namen obdelave, se nanaša na naslednje elemente.

2.2.2 Razsežnosti obveznosti najmanjšega obsega podatkov

48. V členu 25(2) so navedene razsežnosti obveznosti najmanjšega obsega podatkov za privzeto obdelavo, pri čemer je navedeno, da se obveznost uporablja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost.

2.2.2.1 „Količina zbranih osebnih podatkov“

49. Upravljavci bi morali upoštevati obseg osebnih podatkov ter tudi vrste, kategorije in raven podrobnosti osebnih podatkov, potrebnih za namene obdelave. Prav tako bi morali pri svojih odločitvah glede oblikovanja upoštevati čedalje večja tveganja za načela celovitosti in zaupnosti, najmanjši obseg podatkov in omejitev shranjevanja pri zbiranju velikih količin podrobnih osebnih podatkov, ter jih primerjati z manjšimi tveganji pri zbiranju manjših količin in/ali manj podrobnih informacij o posameznikih, na katere se nanašajo osebni podatki. Vsekakor pa privzeta nastavitev ne vključuje zbiranja osebnih podatkov, ki niso potrebni za poseben namen obdelave. Z drugimi besedami, če so posamezne kategorije osebnih podatkov nepotrebne ali če podrobni podatki niso potrebni, ker zadostujejo manj podrobni podatki, se dodatni osebni podatki ne bodo zbirali.

50. Enake zahteve glede privzetega varstva podatkov veljajo za storitve, ki niso odvisne od tega, katera platforma ali naprava se uporablja, pri čemer se lahko zbirajo samo osebni podatki, ki so potrebni za določen namen.

---

[14] Evropski nadzornik za varstvo podatkov. „Smernice za ocenjevanje potrebnosti in sorazmernosti ukrepov, ki omejujejo pravico do varstva podatkov“. 25. februar 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[15] Glej tudi Evropski nadzornik za varstvo podatkov. „Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit“ (Ocenjevanje potrebnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: zbirka orodij). https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[16] Za več informacij o potrebnosti glej Delovno skupino iz člena 29. „Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES“. WP 217, 9. april 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sl.pdf.

2.2.2.2 „Obseg njihove obdelave“

51. Dejanja obdelave,[17] izvedena glede osebnih podatkov, se omejijo na nujno potrebna. K namenu obdelave lahko pripomore več dejanj obdelave, vendar dejstvo, da morajo nekateri osebni podatki izpolniti namen, ne pomeni, da se lahko glede njih izvedejo vse vrste in pogostosti dejanj obdelave. Upravljavci bi morali biti tudi pozorni, da ne širijo meja „združljivih namenov“ iz člena 6(4), in upoštevati, katera obdelava bo še v okviru razumnih pričakovanj posameznikov, na katere se nanašajo osebni podatki.

2.2.2.3 „Obdobje njihove hrambe“

52. Zbrani osebni podatki se ne hranijo, če niso potrebni za namen obdelave ter ni drugega združljivega namena in pravne podlage v skladu s členom 6(4). V skladu z načelom odgovornosti mora upravljavec podatkov po potrebi vsako hrambo objektivno utemeljiti.

53. Upravljavec omeji obdobje hrambe, kolikor je potrebno za ta namen. Če osebni podatki za namen obdelave niso več potrebni, se samodejno izbrišejo ali anonimizirajo. Trajanje obdobja hrambe bo zato odvisno od namena zadevne obdelave. Ta obveznost je neposredno povezana z načelom omejitve shranjevanja iz člena 5(1)(e) in se izvaja samodejno, tj. upravljavec bi moral imeti sistematične postopke za izbris ali anonimizacijo podatkov, vključenih v obdelavo.

54. Anonimizacija[18] osebnih podatkov je alternativa izbrisu, če so upoštevani vsi ustrezni kontekstualni elementi ter se verjetnost in resnost tveganja, vključno s tveganjem za ponovno identifikacijo, redno ocenjujeta.[19]

2.2.2.4 „Njihova dostopnost“

55. Upravljavec bi moral omejiti, kdo in katere vrste dostop ima do osebnih podatkov na podlagi ocene potrebnosti, ter tudi zagotoviti, da so osebni podatki dejansko dostopni osebam, ki in ko to potrebujejo, na primer v kritičnih situacijah. Nadzor dostopa bi bilo treba upoštevati za celotni pretok podatkov med obdelavo.

56. V členu 25(2) je nadalje navedeno, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov brez posredovanja zadevnega posameznika. Upravljavec bi moral samodejno omejiti dostopnost in posamezniku, na katerega se nanašajo osebni podatki, omogočiti posredovanje, preden objavi ali drugače da na voljo osebne podatke o njem nedoločenemu številu posameznikov.

57. Dajanje osebnih podatkov na voljo nedoločenemu številu posameznikov lahko sproži nadaljnje razširjanje podatkov, ki sprva ni bilo predvideno. To je zlasti pomembno v zvezi z internetom in iskalniki. To pomeni, da bi morali upravljavci posameznikom, na katere se nanašajo osebni podatki, samodejno

[17] V skladu s členom 4(2) Splošne uredbe o varstvu podatkov obdelava pomeni zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.
[18] Delovna skupina iz člena 29. „Mnenje št. 5/2014 o anonimizacijskih tehnikah“. WP 216, 10. april 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sl.pdf
[19] Glej člen 4(1) Splošne uredbe o varstvu podatkov, njeno uvodno izjavo 26 in „Mnenje št. 5/2014 Delovne skupine iz člena 29 o anonimizacijskih tehnikah“. Glej tudi pododdelek o „omejitvi shranjevanja“ v oddelku 3 tega dokumenta, ki se nanaša na potrebo, da upravljavec zagotovi učinkovitost izvedenih anonimizacijskih tehnik.

omogočiti, da posredujejo, preden se dajo osebni podatki na voljo na odprtem internetu. To je zlasti pomembno pri otrocih in ranljivih skupinah.

58. Glede na pravno podlago za obdelavo bi se lahko možnost posredovanja razlikovala glede na okoliščine obdelave. Na primer zahteva za privolitev, da postanejo osebni podatki javno dostopni, ali nastavitve zasebnosti, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo, da sami nadzorujejo javni dostop.

59. Tudi v primeru javno dostopnih osebnih podatkov z dovoljenjem in razumevanjem posameznika, na katerega se nanašajo osebni podatki, to ne pomeni, da jih lahko kateri koli drugi upravljavec z dostopom do osebnih podatkov sam prosto obdeluje za svoj namen, ampak mora imeti svojo pravno podlago.[20]

3 IZVAJANJE NAČEL VARSTVA PODATKOV PRI OBDELAVI OSEBNIH PODATKOV Z UPORABO VGRAJENEGA IN PRIVZETEGA VARSTVA PODATKOV

60. Upravljavec bi moral v vseh fazah oblikovanja dejavnosti obdelave, vključno z javnimi naročili, razpisi, oddajanjem del zunanjim izvajalcem, razvojem, podporo, vzdrževanjem, preskušanjem, hrambo, izbrisom itd., upoštevati in preučiti različne elemente vgrajenega in privzetega varstva podatkov, kar bo v tem poglavju ponazorjeno s primeri, umeščenimi v okvir izvajanja načel.[21, 22, 23]

61. Upravljavci morajo izvajati načela za doseganje vgrajenega in privzetega varstva podatkov. Ta načela vključujejo preglednost, zakonitost, pravičnost, omejitev namena, najmanjši obseg podatkov, točnost, omejitev shranjevanja, celovitost in zaupnost ter odgovornost. Navedena so v členu 5 in uvodni izjavi 39 Splošne uredbe o varstvu podatkov. Da bi v celoti razumeli, kako izvajati vgrajeno in privzeto varstvo podatkov, je treba poudariti, kako pomembno je razumeti pomen posameznega načela.

62. Pri predstavitvi primerov, kako konkretizirati vgrajeno in privzeto varstvo podatkov, smo sestavili seznam **ključnih elementov za vgrajeno in privzeto varstvo podatkov** za vsako od načel. Čeprav primeri poudarjajo določeno načelo varstva podatkov, se lahko tudi prekrivajo z drugimi tesno povezanimi načeli. Evropski odbor za varstvo podatkov poudarja, da ključni elementi in primeri, predstavljeni v nadaljevanju, niso niti izčrpni niti zavezujoči, temveč so mišljeni kot smernice za posamezno načelo. Upravljavci morajo oceniti, kako zagotoviti skladnost z načeli v okviru konkretnega zadevnega dejanja obdelave.

63. Čeprav je v tem oddelku poudarek na izvajanju načel, bi moral upravljavec tudi *ustrezno* in *učinkovito* izvajati varstvo pravic posameznikov, na katere se nanašajo osebni podatki, tudi v skladu s poglavjem III Splošne uredbe o varstvu podatkov, če to že ni določeno v samih načelih.

64. Načelo odgovornosti je glavno, saj določa, da mora upravljavec odgovorno izbrati potrebne tehnične in organizacijske ukrepe.

---

[20] Glej zadevo *Satakunnan Markkinapörssi Oy in Satamedia Oy proti Finski*, št. 931/13.

[21] Več primerov je na voljo pri norveškem organu za varstvo podatkov. „Razvoj programske opreme za vgrajeno in privzeto varstvo podatkov“. 28. november 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers.

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

3.1 Preglednost[24]

65. Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, jasno in odkrito pojasniti, kako bo osebne podatke zbiral, uporabljal in delil. Preglednost pomeni omogočanje posameznikom, na katere se nanašajo osebni podatki, da razumejo in po potrebi uveljavijo svoje pravice iz členov od 15 do 22. Načelo je vključeno v člene 12, 13, 14 in 34. Ukrepi in zaščitni ukrepi, uvedeni v podporo načelu preglednosti, bi morali podpirati tudi izvajanje teh členov.

66. Ključni elementi vgrajenega in privzetega varstva podatkov pri načelu preglednosti lahko vključujejo:

- jasnost – informacije morajo biti v jasnem in preprostem jeziku ter jedrnate in razumljive;
- semantiko – komunikacija bi morala imeti jasen pomen za zadevno občinstvo;
- dostopnost – informacije morajo biti posameznikom, na katere se nanašajo osebni podatki, zlahka dostopne;
- kontekstualnost – informacije je treba zagotoviti v ustreznem času in v ustrezni obliki;
- ustreznost – informacije bi morale biti ustrezne in primerne za specifičnega posameznika, na katerega se nanašajo osebni podatki;
- univerzalno oblikovanje – informacije morajo biti dostopne vsem posameznikom, na katere se nanašajo osebni podatki, in vključevati uporabo strojno berljivih jezikov za omogočanje in avtomatizacijo berljivosti in jasnosti;
- razumljivost – posamezniki, na katere se nanašajo osebni podatki, bi morali primerno razumeti, kaj lahko pričakujejo glede obdelave svojih osebnih podatkov, zlasti če so to otroci ali ranljive skupine;
- večkanalnost – informacije je treba poleg besedilne oblike objavljati na različnih kanalih in v različnih medijih, ne le besedilnih, da bi se povečala verjetnost, da učinkovito dosežejo posameznike, na katere se nanašajo osebni podatki;
- večplastnost – informacije bi morale biti večplastne, tako da bi se odpravilo navzkrižje med popolnostjo in razumevanjem, hkrati pa bi se upoštevala razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki.

Primer[25]

Upravljavec na svojem spletišču oblikuje politiko zasebnosti, da bi izpolnil zahteve po preglednosti. Politika zasebnosti ne bi smela vsebovati dolgega dela z informacijami, ki jih povprečen posameznik, na katerega se nanašajo osebni podatki, težko ponotranji in razume. Napisana bi morala biti jasno in jedrnato ter uporabniku spletišča omogočati, da razume, kako se njegovi osebni podatki obdelujejo. Zato upravljavec informacije zagotovi večplastno, pri čemer so najpomembnejše informacije poudarjene. Podrobnejše informacije so zlahka na voljo. Zagotovljeni so spustni seznami in povezave na druge strani za nadaljnje razumevanje različnih točk in pojmov, uporabljenih v politiki. Upravljavec tudi zagotovi, da so informacije posredovane na več kanalih, tudi z videoposnetki za pojasnilo najpomembnejših točk pisnih informacij. Povezanost različnih strani je bistvena za zagotovitev, da se z večplastnim pristopom zmeda ne poveča, ampak zmanjša.

[24] Podrobna opredelitev pojma preglednosti je na voljo v dokumentu Delovne skupine iz člena 29 z naslovom „Smernice o preglednosti na podlagi Uredbe 2016/679“. WP 260 rev. 01, 11. april 2018. https://www.dataprotection-officer.com/image/catalog/dokumenti/wp260rev01_sl.pdf – ki ga je potrdil Evropski odbor za varstvo podatkov.

[25] Francoski organ za varstvo podatkov je objavil več primerov, ki ponazarjajo dobro prakso pri obveščanju uporabnikov in tudi druga načela preglednosti: https://design.cnil.fr/en/.

Politika zasebnosti ne bi smela biti težko dostopna posameznikom, na katere se nanašajo osebni podatki. Zato je na voljo in vidna na vseh spletnih straneh zadevnega spletišča, tako da posameznika, na katerega se nanašajo osebni podatki, od dostopa do informacij loči samo en klik. Zagotovljene informacije so tudi oblikovane v skladu z dobro prakso in standardi za univerzalno oblikovanje, da so dostopne vsem.

Poleg tega bi morale biti potrebne informacije zagotovljene v pravem kontekstu in v ustreznem času. Ker upravljavec veliko dejanj obdelave izvaja z uporabo podatkov, zbranih na spletišču, samo splošna politika zasebnosti na spletišču ne zadostuje, da bi upravljavec izpolnil zahteve po preglednosti. Zato oblikuje tokove informacij, ki posamezniku, na katerega se nanašajo osebni podatki, predstavijo ustrezne informacije v ustreznem kontekstu z uporabo na primer informacijskih izrezkov ali pojavnih elementov. Ko je na primer posameznik, na katerega se nanašajo osebni podatki, zaprošen, da vnese osebne podatke, ga upravljavec obvesti, kako bodo ti obdelani in zakaj so potrebni za obdelavo.

3.2 Zakonitost

67. Upravljavec mora opredeliti veljavno pravno podlago za obdelavo osebnih podatkov. Ukrepi in zaščitni ukrepi bi morali podpirati zahtevo za zagotovitev, da je celoten življenjski cikel obdelave v skladu z ustreznimi pravnimi podlagami obdelave.

68. Ključni elementi vgrajenega in privzetega varstva glede zakonitosti lahko vključujejo:
    - ustreznost – za obdelavo se uporabi pravilna pravna podlaga;
    - razlikovanje[26] – pravna podlaga, ki se uporablja za vsako dejavnost obdelave, se razlikuje;
    - poseben namen – ustrezna pravna podlaga mora biti jasno povezana s posebnim namenom obdelave;[27]
    - potrebnost – obdelava mora biti potrebna in brezpogojna za zakonitost namena;
    - samostojnost – posameznik, na katerega se nanašajo osebni podatki, bi moral imeti najvišjo možno stopnjo samostojnosti glede nadzora nad osebnimi podatki v okvirih pravne podlage;
    - pridobitev privolitve – privolitev mora biti prostovoljna, konkretna, informirana in nedvoumna.[28] Posebno pozornost bi bilo treba nameniti zmožnosti otrok in mladih za prostovoljno informirano privolitev;
    - preklic privolitve – kadar je pravna podlaga privolitev, je treba z obdelavo olajšati preklic privolitve. Preklic mora biti enako preprost kot privolitev. V nasprotnem primeru mehanizem upravljavca za privolitev ni v skladu s Splošno uredbo o varstvu podatkov;[29]
    - uravnoteženje interesov – kadar so pravna podlaga zakoniti interesi, mora upravljavec izvesti tehtano uravnoteženje interesov, pri čemer mora zlasti upoštevati neravnovesje moči, predvsem pri otrocih, mlajših od 18 let, in drugih ranljivih skupinah. Vzpostavljeni so ukrepi in zaščitni ukrepi za ublažitev negativnega vpliva na posameznike, na katere se nanašajo osebni podatki;

[26] Evropski odbor za varstvo podatkov. „Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki“. Različica 2.0, 8. oktober 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[27] Glej oddelek o omejitvi namena v nadaljevanju.

[28] Glej smernice št. 05/2020 o privolitvi v skladu z Uredbo (EU) 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_sl.

[29] Glej smernice št. 05/2020 o privolitvi v skladu z Uredbo (EU) 2016/679, str. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_sl.

- predhodna določitev – pravna podlaga se določi pred obdelavo;
- prenehanje – če pravna podlaga ni več veljavna, se obdelava preneha izvajati;
- prilagoditev – če gre za veljavno spremembo pravne podlage za obdelavo, je treba dejansko obdelavo prilagoditi v skladu z novo pravno podlago;[30]
- razdelitev odgovornosti – kjer je predvideno skupno upravljanje, morajo stranke jasno in pregledno razdeliti svoje zadevne odgovornosti do posameznikov, na katere se nanašajo osebni podatki, ter ukrepe v zvezi z obdelavo oblikovati v skladu s to razdelitvijo.

Primer

Banka načrtuje ponudbo storitve za boljšo učinkovitost obravnave vlog za posojila. Osnovna zamisel storitve je, da lahko banka z zahtevo dovoljenja od stranke pridobi podatke o njej neposredno od javnih davčnih organov. Ta primer ne obravnava obdelave osebnih podatkov drugih virov.

Pridobitev podatkov o finančnem stanju posameznika, na katerega se nanašajo osebni podatki, je potrebna za sprejemanje ukrepov na zahtevo posameznikov, na katere se nanašajo osebni podatki, pred sklenitvijo pogodbe o posojilu.[31] Vendar se šteje, da zbiranje osebnih podatkov neposredno od davčne uprave ni potrebno, saj lahko stranka sklene pogodbo tako, da sama predloži informacije davčne uprave. Čeprav ima lahko banka legitimen interes, da dokumentacijo pridobi neposredno od davčnih organov, na primer za zagotovitev učinkovitosti pri obdelavi posojil, to, da se bankam omogoči tak neposreden dostop do osebnih podatkov prosilcev, pomeni tveganje, povezano z uporabo ali morebitno zlorabo pravic do dostopa.

Pri izvajanju načela zakonitosti se upravljavec zave, da glede tega za del obdelave, ki vključuje zbiranje osebnih podatkov neposredno od javnih organov, ne more uporabiti podlage „potrebnost za izvajanje pogodbe“. Dejstvo, da ta posebna obdelava pomeni tveganje, da bo posameznik, na katerega se nanašajo osebni podatki, manj vključen v obdelavo svojih podatkov, je tudi pomemben dejavnik pri oceni zakonitosti same obdelave. Banka ugotavlja, da mora ta del obdelave temeljiti na drugi pravni podlagi za obdelavo. V določeni državi članici, v kateri ima upravljavec sedež, obstajajo nacionalni zakoni, ki banki dovoljujejo, da informacije zbira neposredno od javnih davčnih organov, če posameznik, na katerega se nanašajo osebni podatki, v to predhodno privoli.

Banka zato predstavi informacije o obdelavi na platformi spletne aplikacije tako, da posameznik, na katerega se nanašajo osebni podatki, zlahka razume, katera obdelava je obvezna in katera neobvezna. Možnosti obdelave samodejno ne dovolijo pridobivanja podatkov neposredno od drugih virov kot samo od posameznikov, na katere se nanašajo osebni podatki, možnost neposrednega pridobivanja podatkov pa je predstavljena tako, da teh posameznikov ne odvrača od tega, da tega ne bi dovolili. Vsaka privolitev za zbiranje podatkov neposredno od drugih upravljavcev je začasna pravica dostopa do specifičnega sklopa informacij.

Vsaka dana privolitev se elektronsko obdela na način, ki ga je mogoče dokumentirati, posameznikom, na katere se nanašajo osebni podatki, pa se predstavi, kako lahko svojo privolitev zlahka nadzorujejo in prekličejo.

Upravljavec je zahteve po vgrajenem in privzetem varstvu predhodno ocenil ter vsa ta merila vključil v svoje specifikacije zahtev za javno naročilo platforme. Upravljavec se zaveda, da če vgrajenega in

[30] Če je izvirna pravna podlaga privolitev, glej smernice št. 05/2020 o privolitvi v skladu z Uredbo (EU) 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_sl.

[31] Glej člen 6(1)(b) Splošne uredbe o varstvu podatkov.

privzetega varstva podatkov ne vključi v javno naročilo, je lahko izvajanje varstva podatkov po tem prepozno ali pa zelo drago.

3.3 Pravičnost

69. Pravičnost je glavno načelo, ki zahteva, da se osebni podatki ne bi smeli obdelati na način, ki je za posameznika, na katerega se nanašajo osebni podatki, neutemeljeno škodljiv, nezakonito diskriminacijski, nepričakovan ali zavajajoč. Ukrepi in zaščitni ukrepi, s katerimi se izvaja načelo pravičnosti, podpirajo tudi pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zlasti pravico do obveščenosti (preglednost), pravico do posredovanja (dostop, izbris, prenosljivost podatkov, popravki) in pravico do omejitve obdelave (pravica, da zanje ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, in nediskriminacijo posameznikov, na katere se nanašajo osebni podatki v takih postopkih).

70. Ključni elementi vgrajenega in privzetega varstva v zvezi s pravičnostjo lahko vključujejo:
    - samostojnost – posameznikom, na katere se nanašajo osebni podatki, je treba zagotoviti najvišjo možno stopnjo samostojnosti pri določanju uporabe svojih osebnih podatkov ter glede obsega in pogojev te uporabe ali obdelave;
    - interakcijo – posamezniki, na katere se nanašajo osebni podatki, morajo biti sposobni komunicirati in uresničevati svoje pravice v zvezi z osebnimi podatki, ki jih obdeluje upravljavec;
    - pričakovanja – obdelava bi morala ustrezati razumnim pričakovanjem posameznikov, na katere se nanašajo osebni podatki;
    - nediskriminacijo – upravljavec ne sme nepravično diskriminirati posameznikov, na katere se nanašajo osebni podatki;
    - neizkoriščanje – upravljavec ne bi smel izkoriščati potreb ali ranljivosti posameznikov, na katere se nanašajo osebni podatki;
    - potrošnikovo izbiro – upravljavec ne bi smel nepravično „vezati“ svojih uporabnikov. Kadar je storitev, ki obdeluje osebne podatke, pravno zaščitena, lahko ustvari vezanost na storitev, kar morda ni pravično, če to ovira možnost posameznikov, na katere se nanašajo osebni podatki, da uveljavljajo svojo pravico do prenosljivosti podatkov v skladu s členom 20;
    - ravnovesje moči – ravnovesje moči bi moral biti glavni cilj razmerja med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki. Neravnovesja moči bi bilo treba preprečiti. Če to ni mogoče, bi jih bilo treba priznati in jih obravnavati z ustreznimi protiukrepi;
    - neprenos tveganja – upravljavci ne bi smeli prenesti tveganj podjetja na posameznika, na katerega se nanašajo osebni podatki;
    - nezavajanje – informacije o obdelavi podatkov in možnosti obdelave podatkov bi bilo treba zagotoviti objektivno in nevtralno, pri čemer se je treba izogibati zavajajočemu ali manipulativnemu jeziku ali obliki;
    - spoštovanje pravic – upravljavec mora spoštovati temeljne pravice posameznikov, na katere se nanašajo osebni podatki, ter izvajati ustrezne ukrepe in zaščitne ukrepe, pri čemer v te pravice ne sme posegati, razen če je to izrecno zakonsko utemeljeno;
    - etičnost – upravljavec bi moral razumeti širši vpliv obdelave na posameznikove pravice in dostojanstvo;
    - verodostojnost – upravljavec bi moral dati na voljo informacije o načinu obdelave osebnih podatkov in ravnati v skladu s svojo izjavo o ravnanju ter ne bi smel zavajati posameznikov, na katere se nanašajo osebni podatki;

- človeško posredovanje – upravljavec mora vključiti *prilagojeno* človeško posredovanje, ki je sposobno odkriti pristranskost strojne obdelave v skladu s pravico posameznika iz člena 22, da zanj ne velja odločitev, ki temelji le na avtomatizirani obdelavi;[32]
- pravične algoritme – redno se ocenjuje, ali algoritmi delujejo v skladu z nameni, in prilagaja algoritme tako, da blažijo odkrite pristranskosti ter zagotavljajo pravičnost pri obdelavi. Posameznikom, na katere se nanašajo osebni podatki, bi bilo treba zagotoviti informacije o tem, kako deluje obdelava osebnih podatkov na podlagi algoritmov za analizo ali predvidevanje njihove uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa ali interesov, zanesljivosti ali vedenja, lokacije ali gibanja.[33]

Primer 1

Upravljavec upravlja iskalnik, s katerim se obdelujejo zlasti osebni podatki uporabnika. Upravljavec ima korist od velike količine osebnih podatkov in možnosti, da te osebne podatke uporabi za ciljno oglaševanje. Zato želi vplivati na posameznike, na katere se nanašajo osebni podatki, da mu dovolijo obsežnejše zbiranje in uporabo svojih osebnih podatkov. Privolitev je treba pridobiti tako, da se posamezniku, na katerega se nanašajo osebni podatki, predstavijo možnosti obdelave.

Pri izvajanju načela pravičnosti ter ob upoštevanju narave, obsega, okoliščin in namenov obdelave se upravljavec zaveda, da ti ne morejo predstaviti možnosti tako, da bi posameznika, na katerega se nanašajo osebni podatki, usmerjali k dovoljenju, da upravljavec zbere več osebnih podatkov kot, če bi bile možnosti predstavljane enakovredno in nevtralno. To pomeni, da ne morejo predstaviti dejanj obdelave tako, da bi posamezniki, na katere se nanašajo osebni podatki, težko izmenjali svoje podatke ali težko prilagodili svoje nastavitve zasebnosti in omejili obdelavo. To so primeri zavajanj, ki so v nasprotju z bistvom člena 25. Zato bi morale biti privzete možnosti za obdelavo čim bolj nevtralne, odločitev za nadaljnjo obdelavo pa bi morala biti predstavljena tako, da posameznike, na katere se nanašajo osebni podatki, ne sili k privolitvi. Zato upravljavec predstavi možnosti privolitve ali vzdržanja kot dve enako vidni izbiri, ki posamezniku, na katerega se nanašajo osebni podatki, natančno predstavita posledice posamezne izbire.

Primer 2

Drug upravljavec obdeluje osebne podatke za zagotavljanje storitve pretakanja, pri kateri uporabniki lahko izbirajo med redno naročnino standardne kakovosti in višjo naročnino (*premium*) za boljšo kakovost. Kot del naročnine *premium* naročniki dobijo prednostno storitev za stranko.

Glede na načelo pravičnosti prednostna storitev za stranko, odobrena naročnikom z višjo naročnino, ne sme diskriminirati dostopa rednih naročnikov do uveljavljanja njihovih pravic v skladu s členom 12 Splošne uredbe o varstvu podatkov. To pomeni, da čeprav naročniki z višjo naročnino dobijo prednostno storitev, taka prednost ne sme povzročiti, da rednim naročnikom zaradi pomanjkanja

[32] Glej smernice o avtomatiziranem sprejemanju posameznih odločitev in oblikovanju profilov za namene Uredbe (EU) 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Glej uvodno izjavo 71 Splošne uredbe o varstvu podatkov.

ustreznih ukrepov ne bi odgovorili na njihovo zahtevo brez nepotrebnega odlašanja, vsekakor pa v enem mesecu po prejemu zahtev.

Prednostne stranke sicer lahko plačajo za boljšo storitev, vendar pa imajo vsi posamezniki, na katere se nanašajo osebni podatki, enak in enakopraven dostop za uresničevanje svojih pravic in svoboščin v skladu s členom 12.

3.4 Omejitev namena[34]

71. Upravljavec mora zbirati podatke za določene, izrecne in zakonite namene ter jih ne sme nadalje obdelovati na način, ki ni združljiv s temi nameni.[35] Obdelava bi torej morala biti oblikovana glede na to, kaj je potrebno za doseganje namenov. Če bo potekala nadaljnja obdelava, mora upravljavec najprej zagotoviti, da so nameni te obdelave združljivi s prvotnimi nameni, in tako obdelavo ustrezno oblikovati. Ali je nov namen združljiv ali ne, se oceni po merilih iz člena 6(4).

72. Ključni elementi vgrajenega in privzetega varstva glede omejitve namena lahko vključujejo:
- predhodno določitev – zakoniti nameni se določijo pred oblikovanjem obdelave;
- specifičnost – namen je natančno opredeljen in pojasnjuje, zakaj se osebni podatki obdelujejo;
- usmerjenost na namen – namen obdelave mora usmerjati oblikovanje obdelave in določati meje obdelave;
- potrebnost – namen določa, katere osebne podatke je treba obdelati;
- združljivost – nov namen mora biti združljiv s prvotnim namenom, za katerega so se zbirali podatki, in usmerjati ustrezne spremembe pri oblikovanju;
- omejitev nadaljnje obdelave – upravljavec ne sme povezovati naborov podatkov ali izvajati nadaljnje obdelave za nove nezdružljive namene;
- omejitev ponovne uporabe – upravljavec bi moral uporabiti tehnične ukrepe, vključno z zgoščevalno funkcijo (*hash*) ali šifriranjem, da omeji možnost spremembe namena obdelave osebnih podatkov. Upravljavec bi moral imeti tudi organizacijske ukrepe, kot so politike in pogodbene obveznosti, ki omejujejo ponovno uporabo osebnih podatkov;
- pregled – upravljavec bi moral redno pregledovati, ali je obdelava potrebna za namene, za katere so se zbirali podatki, in preskušati oblikovanje glede omejitve namena.

Primer

Upravljavec obdeluje osebne podatke o svojih strankah. Namen obdelave je izpolnitev pogodbe, to je sposobnost dobaviti blago na pravi naslov in za to dobiti plačilo. Shranjeni osebni podatki so zgodovina nakupa, ime, naslov in e-naslov ter telefonska številka kupca.

Upravljavec razmišlja, da bi kupil opremo za upravljanje odnosov s strankami (CRM), ki zbira vse podatke o stranki, in sicer o prodaji, trženju in storitvi za stranko, na enem mestu. Ta oprema omogoča shranjevanje vseh telefonskih klicev, dejavnosti, dokumentov, e-pošte in trženjskih akcij za pridobitev 360-stopinjskega pogleda na stranko. Poleg tega lahko ta oprema samodejno analizira kupno moč

[34] Delovna skupina iz člena 29 je zagotovila smernice za razumevanje načela omejitve namena na podlagi Direktive 95/46/ES. Čeprav Evropski odbor za varstvo podatkov tega mnenja ni sprejel, pa je še vedno pomembno, saj je besedilo načela enako kot v Splošni uredbi o varstvu podatkov. Delovna skupina iz člena 29. „Mnenje št. 03/2013 o omejitvi namena“. WP 203, 2. april 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Člen 5(1)(b) Splošne uredbe o varstvu podatkov.

strank z uporabo javnih informacij. Namen analize je boljše ciljno usmerjanje oglaševalskih dejavnosti, ki pa niso del prvotnega zakonitega namena obdelave.

Zaradi spoštovanja načela omejitve namena upravljavec od ponudnika opreme zahteva, da razporedi različne dejavnosti obdelave, pri katerih se uporabljajo osebni podatki, po namenih, pomembnih za upravljavca.

Ko upravljavec prejme rezultate razporejanja, oceni, ali sta novi namen trženja in namen ciljnega oglaševanja združljiva s prvotnimi nameni, opredeljenimi ob zbiranju podatkov, in ali obstaja zadostna pravna podlaga za zadevno obdelavo. Če ocena ne da pritrdilnega odgovora, upravljavec ne nadaljuje uporabe zadevnih funkcij. Druga možnost je, da se upravljavec odpove oceni in opisanih funkcij opreme preprosto ne uporabi.

3.5 Najmanjši obseg podatkov

73. Obdelujejo se samo osebni podatki, ki so ustrezni, relevantni in omejeni na to, kar je **potrebno** za namen.[36] Zato mora upravljavec vnaprej določiti, katere značilnosti in parametri sistemov za obdelavo in njihove podporne funkcije so dovoljeni. Najmanjši obseg podatkov utemeljuje in konkretizira načelo potrebnosti. Pri nadaljnji obdelavi bi moral upravljavec redno presojati, ali so obdelani osebni podatki še vedno ustrezni, relevantni in potrebni ali pa bodo izbrisani ali anonimizirani.

74. Upravljavci bi morali najprej določiti, ali je sploh treba, da obdelujejo osebne podatke za ustrezne namene. Upravljavec bi moral preveriti, ali je mogoče ustrezne namene doseči z obdelavo manjšega števila osebnih podatkov ali z manj podrobnimi ali združenimi osebnimi podatki ali brez obdelave osebnih podatkov.[37] Tako preverjanje bi bilo treba izvesti pred obdelavo, lahko pa tudi kadar koli v življenjskem ciklu obdelave. To je tudi v skladu s členom 11.

75. Najmanjši obseg se lahko nanaša tudi na stopnjo identifikacije. Če namen obdelave ne zahteva, da se končni nabor podatkov nanaša na določenega ali določljivega posameznika (kot je to v statistiki), temveč to zahteva začetna obdelava (na primer pred združevanjem podatkov), upravljavec izbriše ali anonimizira osebne podatke takoj, ko identifikacija ni več potrebna. Če je nadaljnja identifikacija potrebna za druge obdelave, bi morali biti osebni podatki psevdonimizirani, da se zmanjšajo tveganja za pravice posameznikov, na katere se nanašajo osebni podatki.

76. Ključni elementi vgrajenega in privzetega varstva v zvezi z najmanjšim obsegom podatkov lahko vključujejo:
    - izogibanje obdelavi – izogibati se je treba obdelavi osebnih podatkov v celoti, če je to mogoče za ustrezen namen;
    - omejitev – omejiti količino zbranih osebnih podatkov na to, kar je potrebno za namen;
    - omejitev dostopa – obdelava podatkov se oblikuje tako, da dostop do osebnih podatkov za opravljanje svojih nalog potrebuje čim manjše število oseb, pri čemer se dostop ustrezno omeji;
    - ustreznost – osebni podatki bi morali biti ustrezni za zadevno obdelavo, upravljavec pa bi moral biti zmožen to ustreznost dokazati;

[36] Člen 5(1)(c) Splošne uredbe o varstvu podatkov.
[37] V uvodni izjavi 39 Splošne uredbe o varstvu podatkov je navedeno: „Osebni podatki bi se lahko obdelali le, če namena obdelave ne bi bilo mogoče razumno doseči z drugimi sredstvi.“

- potrebnost – vsaka kategorija osebnih podatkov je potrebna za določen namen in mora biti obdelana le, če tega ni mogoče izpolniti z drugimi sredstvi;
- združevanje – če je mogoče, uporabiti združene podatke;
- psevdonimizacijo – psevdonimizirati osebne podatke, takoj ko neposredno določljivi osebni podatki niso več potrebni, in posebej shraniti identifikacijske ključe;
- anonimizacijo in izbris – če osebni podatki niso ali niso več potrebni za namen, se anonimizirajo ali izbrišejo;
- pretok podatkov – pretok podatkov bi moral biti dovolj učinkovit, da se ne ustvari več kopij, kot je potrebno;
- „najnovejši tehnološki razvoj“ – upravljavec bi moral uporabiti najnovejše in ustrezne tehnologije, da se izogne obdelavi podatkov in zagotovi najmanjši obseg.

Primer 1

Knjigarna želi povečati svoj dohodek s spletno prodajo knjig. Njen lastnik želi za naročanje vzpostaviti standardiziran obrazec. Da bi zagotovil, da stranke izpolnijo vse informacije, ki jih želi pridobiti, je vsa polja označil kot obvezna (če stranka ne izpolni vseh, naročila ne more poslati). Lastnik spletne knjigarne je naprej uporabljal standardni kontaktni obrazec, v katerega mora stranka vpisati informacije, med drugim datum rojstva, telefonsko številko in domači naslov. Vendar vsa polja na obrazcu niso potrebna za namen nakupa in dostave knjig. Če posameznik, na katerega se nanašajo osebni podatki, v tem posebnem primeru izdelek plača vnaprej, datum rojstva in telefonska številka za nakup izdelka nista potrebna. To pomeni, da za naročilo izdelka ni mogoče zahtevati, da se ti polji izpolnita, razen če lahko upravljavec jasno dokaže, da je to kako drugače potrebno in zakaj sta polji potrebni. Poleg tega so tudi primeri, pri katerih naslov ni potreben. Pri naročilu e-knjige lahko stranka na primer izdelek prenese neposredno na svojo napravo.

Zato se lastnik knjigarne odloči, da bo pripravil dva spletna obrazca, enega za naročanje knjig s poljem za vnos naslova stranke in enega za naročanje e-knjig brez polja za naslov stranke.

Primer 2

Družba za javni prevoz želi zbrati informacije na podlagi načrtov potovanja. To je koristno za namene ustreznih odločitev o spremembi voznih redov javnega prevoza in ustreznega določanja poti za vlake. Potniki morajo svoje vozovnice vstaviti v čitalnik vsakič, ko v prevozno sredstvo vstopijo ali iz njega izstopijo. Upravljavec je opravil oceno tveganja v zvezi s pravicami in svoboščinami potnikov glede zbiranja njihovih načrtov potovanja ter ugotavlja, da je mogoče potnike, če živijo ali delajo na redko poseljenih območjih, zaradi identifikatorja vozovnice identificirati na podlagi identifikacije posamezne proge. Zato upravljavec ne shrani identifikatorja vozovnice, ker ni potreben za namen izboljšanja voznega reda javnega prevoza in določanja poti vlakov. Po končanem potovanju upravljavec shrani samo posamezne načrte potovanja, tako da ni mogoče identificirati potovanj, povezanih z eno samo vozovnico, ampak obdrži samo informacijo o ločenih načrtih potovanja.

V primerih, ko še vedno obstaja tveganje identifikacije osebe le prek njenega načrta poti v javnem prevozu, upravljavec izvaja statistične ukrepe za zmanjšanje tveganja, kot je izločanje začetka in konca potovanja.

Primer 3

Kurirska služba želi oceniti učinkovitost svojih dostav s stališča dostavnih rokov, razporeda delovne obremenitve in porabe goriva. Za izpolnitev tega cilja mora obdelati številne osebne podatke v zvezi z zaposlenimi (vozniki) in strankami (naslovi, pošiljke, ki jih je treba dostaviti itd.). To dejanje obdelave povzroči tveganja za spremljanje zaposlenih, za kar so potrebni posebni pravni zaščitni ukrepi, in sledenje navadam stranke s poznavanjem dostavljenih pošiljk skozi čas. Ta tveganja je mogoče močno zmanjšati z ustrezno psevdonimizacijo zaposlenih in strank. Zlasti če se ključi za psevdonimizacijo pogosto menjajo in se namesto natančnih naslovov upoštevajo makro območja, gre za učinkovit najmanjši obseg podatkov, upravljavec pa se lahko osredotoči samo na dostavo in namen izboljšanja virov, ne da bi presegel prag spremljanja vedenja posameznikov (strank ali zaposlenih).

Primer 4

Bolnišnica zbira podatke o svojih pacientih v bolnišničnem informacijskem sistemu (elektronski zdravstveni zapis). Bolnišnično osebje mora dostopati do dokumentacije pacientov, da lahko sprejme informirane odločitve glede njihove oskrbe in zdravljenja ter evidentira vsa dejanja glede diagnostike, oskrbe in zdravljenja. Dostop imajo samodejno omogočen samo člani zdravstvenega osebja, ki jim je dodeljeno zdravljenje zadevnega pacienta v specialističnem oddelku. Skupina oseb z dostopom do dokumentacije pacienta se razširi, če pri zdravljenju sodelujejo drugi oddelki ali diagnostične enote. Ko je pacient odpuščen in je obračun končan, se dostop omeji na majhno skupino zaposlenih na posamezen specialistični oddelek, ki odgovarjajo na zahteve po zdravstvenih informacijah ali posvetovanje, ki ga opravijo ali zanj prosijo drugi ponudniki zdravstvenih storitev po pooblastilu zadevnega pacienta.

3.6 Točnost

77. Osebni podatki morajo biti točni in po potrebi posodobljeni; uporabijo se vsi primerni ukrepi za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo.[38]

78. Zahteve bi bilo treba razumeti v zvezi s tveganji in posledicami za konkretno uporabo podatkov. Netočni osebni podatki lahko pomenijo tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ker na primer pripeljejo do napačne diagnoze ali napačne obdelave zdravstvenega protokola, ali pa lahko napačna slika osebe vodi do odločitev na napačni podlagi, ki se sprejemajo ročno, avtomatizirano ali prek umetne inteligence.

79. Ključni elementi vgrajenega in privzetega varstva glede točnosti lahko vključujejo:
    - vir podatkov – viri osebnih podatkov bi morali biti zanesljivi v smislu točnosti podatkov;
    - stopnjo točnosti – vsak element osebnega podatka bi moral biti tako točen, kot je potrebno za posebne namene;
    - izmerljivo točnost – zmanjša se število lažno pozitivnih/negativnih rezultatov, na primer pristranskosti v avtomatiziranih odločitvah in umetni inteligenci;

[38] Člen 5(1)(d) Splošne uredbe o varstvu podatkov.

- preverjanje – upravljavec mora odvisno od narave podatkov v zvezi s pogostostjo njihove spremembe preveriti pravilnost osebnih podatkov pri posameznikih, na katere se nanašajo osebni podatki, pred različnimi fazami obdelave in ob njih (na primer zahteve glede starosti);
- izbris/popravek – upravljavec nemudoma izbriše ali popravi netočne podatke. Upravljavec to zlasti olajša, če so ali so bili posamezniki, na katere se nanašajo osebni podatki, otroci in pozneje želijo take osebne podatke odstraniti;[39]
- preprečitev širjenja napak – upravljavci bi morali ublažiti učinek akumulirane napake v obdelovalni verigi;
- dostop – posamezniki, na katere se nanašajo osebni podatki, bi morali dobiti informacije in učinkovit dostop do osebnih podatkov v skladu s členi 12 do 15 Splošne uredbe o varstvu podatkov, da bi po potrebi nadzorovali njihovo točnost in jih popravili;
- nenehno točnost – osebni podatki bi morali biti točni v vseh fazah obdelave, v kritičnih fazah pa bi bilo treba opraviti preskus točnosti;
- posodobljenost – osebni podatki morajo biti posodobljeni, če je to potrebno za namen;
- zasnovo podatkov – uporabijo se tehnološke in organizacijske značilnosti zasnove, da bi se zmanjšala netočnost, na primer predstavitev jedrnatih vnaprej določenih možnosti namesto polj za prosto besedilo.

Primer 1

Zavarovalnica želi uporabiti umetno inteligenco za oblikovanje profilov strank, ki kupujejo zavarovanje, kot podlago za svoje odločanje pri izračunu zavarovalnega tveganja. Pri določitvi načina razvoja rešitev umetne inteligence določa načine obdelave in bi morala pri izbiri aplikacije z umetno inteligenco pri prodajalcu in odločanju, kako učiti umetno inteligenco, upoštevati vgrajeno varstvo podatkov.

Upravljavec bi moral pri določitvi, kako učiti umetno inteligenco, imeti točne podatke, da dobi točne rezultate. Zato bi moral zagotoviti, da so podatki, ki se uporabijo za učenje umetne inteligence, točni.

Če ima veljavno pravno podlago za učenje umetne inteligence z uporabo osebnih podatkov iz velike podskupine svojih obstoječih strank, upravljavec izbere skupino strank, ki je reprezentativna za populacijo, da se izogne tudi pristranskosti.

Podatki o strankah se nato zberejo iz ustreznega sistema za obdelavo podatkov, vključno s podatki o vrsti zavarovanja, na primer zdravstveno zavarovanje, zavarovanje doma, potovalno zavarovanje itd., ter podatki iz javnih registrov, do katerih imajo zakonit dostop. Vsi podatki se psevdonimizirajo, preden se prenesejo v sistem, namenjen učenju modela umetne inteligence.

Da bi zagotovili, da so podatki, uporabljeni za učenje umetne inteligence, čim bolj točni, upravljavec zbira podatke iz virov s pravilnimi in posodobljenimi informacijami.

Zavarovalnica preveri, ali je umetna inteligenca zanesljiva in zagotavlja nediskriminatorne rezultate tako med njenim razvojem kot tudi pred njeno izdajo. Ko je umetna inteligenca v celoti usposobljena in deluje, zavarovalnica uporabi rezultate za podporo ocenam zavarovalnega tveganja, vendar se pri odločanju o odobritvi zavarovanja ne zanaša zgolj na umetno inteligenco, razen če je odločitev sprejeta v skladu z izjemami iz člena 22(2) Splošne uredbe o varstvu podatkov.

Zavarovalnica bo tudi redno pregledovala rezultate umetne inteligence, da bi ohranila zanesljivost in po potrebi prilagodila algoritem.

[39] Glej uvodno izjavo 65.

Primer 2

Upravljavec je zdravstvena ustanova, ki želi najti metode za zagotavljanje celovitosti in točnosti osebnih podatkov v registrih svojih pacientov.

V primerih, ko dve osebi hkrati prideta v ustanovo in sta enako zdravljeni, obstaja tveganje njune zamenjave, če je ime edini parameter za njuno razlikovanje. Upravljavec za zagotavljanje točnosti potrebuje edinstveno oznako za posamezno osebo in torej več informacij kot samo ime pacienta.

Ustanova uporablja različne sisteme, ki vsebujejo osebne informacije o pacientih, ter mora zagotoviti, da je informacija v zvezi z njimi kadar koli v vseh sistemih pravilna, točna in dosledna. Ustanova je opredelila različna tveganja, ki se lahko pojavijo, če se informacija spremeni v enem sistemu, ne pa v drugih.

Upravljavec se odloči, da bo zmanjšal tveganje z uporabo zgoščevalne funkcije (*hash*), ki se lahko uporabi za zagotavljanje celovitosti podatkov v dnevniku zdravljenja. Za zapise dnevnika zdravljenja in pacienta, ki je z njimi povezan, se ustvarijo nespremenljivi časovni žigi, tako da je mogoče po potrebi vse spremembe prepoznati, jih postaviti v vzajemno zvezo in jim slediti.

3.7 Omejitev shranjevanja

80. Upravljavec mora zagotoviti, da so osebni podatki hranjeni v obliki, ki dovoljuje identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo.[40]
Bistveno je, da upravljavec točno ve, katere osebne podatke podjetje obdeluje in zakaj. Namen obdelave je glavno merilo pri odločanju, kako dolgo se bodo osebni podatki hranili.

81. Ukrepi in zaščitni ukrepi, s katerimi se izvaja načelo omejitve shranjevanja, dopolnjujejo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, natančneje pravico do izbrisa in pravico do ugovora.

82. Ključni elementi vgrajenega in privzetega varstva glede omejitve shranjevanja lahko vključujejo:
- izbris in anonimizacijo – upravljavec bi moral imeti jasne notranje postopke in funkcije za izbris in/ali anonimizacijo;
- učinkovitost anonimizacije/izbrisa – upravljavec mora zagotoviti, da ni mogoče ponovno identificirati anonimiziranih podatkov ali izbrisanih podatkov obnoviti, in bi moral preskusiti, ali je to mogoče;
- avtomatizacijo – izbris nekaterih osebnih podatkov bi moral biti avtomatiziran;
- merila za hrambo – upravljavec določi, kateri podatki in kakšno trajanje hrambe so potrebni za namen;
- utemeljitev – upravljavec je sposoben utemeljiti, zakaj je obdobje hrambe potrebno za namen in zadevne osebne podatke, ter razkriti utemeljitev in pravno podlago za obdobje hrambe;
- izvrševanje politik hrambe – upravljavec bi moral izvrševati notranje politike hrambe in izvajati preizkuse, ali organizacija svoje politike izvaja;
- varnostne kopije/dnevnike – upravljavec določi, kateri podatki in kakšno trajanje hrambe so potrebni za varnostne kopije in dnevnike;

[40] Člen 5(1)(c) Splošne uredbe o varstvu podatkov.

- pretok podatkov – upravljavci bi morali biti pozorni na pretok osebnih podatkov in shranjevanje njihovih kopij ter si prizadevati za omejitev njihove „začasne“ hrambe.

Primer

Upravljavec zbira osebne podatke, kadar je namen obdelave upravljanje članstva posameznika, na katerega se nanašajo osebni podatki. Osebni podatki se izbrišejo, ko se članstvo prekine in za nadaljnjo hrambo podatkov ni pravne podlage.

Upravljavec najprej pripravi notranji postopek za hrambo in izbris podatkov. V skladu s tem zaposleni osebne podatke po končanem obdobju hrambe ročno izbrišejo. Zaposleni upošteva postopek za redno brisanje in popravke podatkov iz vseh naprav, varnostnih kopij, dnevnikov, e-poštnih sporočil in drugih ustreznih nosilcev shranjevanja.

Da bi bil izbris učinkovitejši in manj nagnjen k napakam, upravljavec nato namesto tega uvede samodejni sistem za samodejno, zanesljivo in še bolj redno brisanje podatkov. Sistem je nastavljen za spremljanje danega postopka za izbris podatkov, ki se potem izvede ob vnaprej določenih rednih časovnih presledkih in odstrani osebne podatke z vseh nosilcev shranjevanja v podjetju. Upravljavec redno pregleduje in preskuša postopek hrambe ter zagotovi, da se hramba izvaja v skladu s posodobljeno politiko hrambe.

3.8 Celovitost in zaupnost

83. Načelo celovitosti in zaupnosti vključuje zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo, in sicer z ustreznimi tehničnimi ali organizacijskimi ukrepi. Za varnost osebnih podatkov so potrebni ustrezni ukrepi za preprečevanje in obvladovanje kršitev varstva podatkov, zagotavljanje pravilnega izvajanja nalog obdelave podatkov in skladnosti z drugimi načeli ter olajšanje učinkovitega uveljavljanja pravic posameznikov.

84. V uvodni izjavi 78 je navedeno, da je lahko eden od ukrepov vgrajenega in privzetega varstva podatkov, da upravljavec *„vzpostavi in izboljša varnostne ukrepe“*. Skupaj z drugimi ukrepi vgrajenega in privzetega varstva podatkov je v uvodni izjavi 78 navedena odgovornost, da upravljavec stalno ocenjuje, ali ves čas uporablja ustrezna sredstva obdelave in ali izbrani ukrepi dejansko preprečujejo obstoječe ranljivosti. Nadalje, upravljavci bi morali izvajati redne preglede ukrepov informacijske varnosti, ki obdajajo in varujejo osebne podatke, ter postopka za obravnavo kršitev varstva podatkov.

85. Ključni elementi vgrajenega in privzetega varstva glede celovitosti in zaupnosti lahko vključujejo:
    - sistem upravljanja informacijske varnosti (ISMS) – imeti operativna sredstva za upravljanje politik in postopkov informacijske varnosti.
    - analizo tveganja – oceniti tveganja glede na varnost osebnih podatkov ob upoštevanju vpliva na pravice posameznikov in preprečevati opredeljena tveganja. Za uporabo pri oceni tveganja; razviti in vzdrževati celovito, sistematično in realistično „modeliranje groženj“ ter analizo možnih tarč napada v okviru načrtovane programske opreme, da se zmanjšajo napadni vektorji ter priložnosti za izkoriščanje šibkih točk in ranljivosti;
    - vgrajeno varnost – čim prej preučiti varnostne zahteve pri zasnovi in razvoju sistema ter stalno vključevati in izvajati ustrezne preskuse;
    - vzdrževanje – redno pregledovati in preskušati programsko opremo, strojno opremo, sisteme, storitve itd., da se odkrijejo ranljivosti sistemov, ki podpirajo obdelavo;

- upravljanje nadzora dostopa – dostop do osebnih podatkov, potrebnih za naloge obdelave, bi moralo imeti samo osebje, ki ga potrebuje, upravljavec pa bi moral razlikovati med privilegiji za dostop pooblaščenega osebja;
    - omejitev dostopa (agenti) – obdelava podatkov se oblikuje tako, da dostop do osebnih podatkov za opravljanje svojih nalog potrebuje čim manjše število oseb, pri čemer se dostop ustrezno omeji;
    - omejitev dostopa (vsebina) – v okviru vsakega dejanja obdelave omejiti dostop samo na atribute na podatkovni niz, ki so potrebni za izvedbo tega dejanja. Poleg tega je treba omejiti dostop do podatkov, ki so povezani s posamezniki, na katere se nanašajo osebni podatki, ki so v pristojnosti zadevnega zaposlenega;
    - ločevanje dostopa – obdelavo podatkov je treba oblikovati tako, da noben posameznik ne potrebuje celovitega dostopa do vseh zbranih podatkov o posamezniku, na katerega se nanašajo osebni podatki, in še manj do vseh osebnih podatkov posamezne kategorije posameznikov, na katere se nanašajo osebni podatki;
- varne prenose – prenosi so zavarovani pred nepooblaščenim in nenamernim dostopom in spremembami;
- varno hrambo – shranjevanje podatkov je zavarovano pred nepooblaščenim dostopom in spremembami. Vzpostavljeni so postopki za oceno tveganja centraliziranega ali decentraliziranega shranjevanja in tega, na katere osebne podatke se to nanaša. Za nekatere podatke bodo morda potrebni dodatni varnostni ukrepi ali ločitev od drugih osebnih podatkov;
- psevdonimizacijo – osebni podatki in varnostne kopije/dnevniki bi morali biti psevdonimizirani kot varnostni ukrep za zmanjšanje tveganja morebitnih kršitev varstva podatkov, na primer z uporabo zgoščevalne funkcije in šifriranja;
- varnostne kopije/dnevnike – hraniti varnostne kopije in dnevnike, v obsegu, potrebnem za informacijsko varnost, uporabiti revizijske sledi in spremljanje dogodka kot rutinski varnostni nadzor. Te je treba zaščititi pred nepooblaščenim in nenamernim dostopom in spremembami ter jih redno pregledovati, incidente pa je treba nemudoma obravnavati;
- vnovično vzpostavitev delovanja po nepredvidljivih dogodkih/neprekinjeno poslovanje – obravnavati zahteve glede vnovične vzpostavitve delovanja po nepredvidljivih dogodkih in neprekinjenega poslovanja za povrnitev razpoložljivosti osebnih podatkov po resnih incidentih;
- varstvo glede na tveganje – vse kategorije osebnih podatkov bi bilo treba zaščititi z ukrepi, ki ustrezajo tveganju kršitve varstva. Podatke, ki pomenijo posebno tveganje, bi bilo treba po možnosti hraniti ločeno od preostalih osebnih podatkov;
- upravljanje odzivanja na varnostne incidente – vzpostaviti je treba načine, postopke in sredstva za odkrivanje, zajezitev, obravnavanje, poročanje in učenje iz kršitev varstva podatkov;
- upravljanje incidentov – upravljavec bi moral imeti vzpostavljene postopke za obravnavanje kršitev in incidentov, da bi bil sistem obdelave zanesljivejši. To vključuje postopke obveščanja, kot je upravljanje obveščanja (nadzornega organa) in sporočanja (posameznikom, na katere se nanašajo osebni podatki).

Primer

Upravljavec želi iz zdravstvene zbirke podatkov, ki vsebuje elektronsko zdravstveno kartoteko (pacienta), izluščiti velike količine osebnih podatkov in jih prenesti v namenski strežnik podatkovne zbirke v podjetju, da bi obdelal izvlečene podatke za namene zagotavljanja kakovosti. Podjetje je ocenilo tveganje za usmerjanje ekstrakcij na strežnik, dostopen vsem zaposlenim v podjetju, kot verjetno visoko za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Ker je v

podjetju samo en oddelek, ki mora obdelati izvlečke podatkov o pacientih, se upravljavec odloči, da bo dostop do namenskega strežnika omejil na zaposlene v tem oddelku. Da bi tveganje še bolj zmanjšal, bo podatke pred prenosom tudi psevdonimiziral.

Da bi podjetje uredilo dostop in zmanjšalo morebitno škodo zlonamerne programske opreme, se odloči, da izloči omrežje ter vzpostavi nadzor dostopa do strežnika. Poleg tega vzpostavi spremljanje varnosti in odkrivanje vdora ter sistem preprečevanja in ga loči od redne uporabe. Za spremljanje dostopa in sprememb se vzpostavi samodejni sistem revizije. Če se nastavijo nekateri dogodki, povezani z uporabo, se iz tega ustvarijo poročila in samodejna opozorila. Upravljavec bo zagotovil, da imajo uporabniki dostop samo na podlagi potrebe po seznanitvi in ustrezno raven dostopa. Neustrezno uporabo je mogoče hitro in zlahka odkriti.

Nekatere izvlečke je treba primerjati z novimi in jih je zato treba hraniti tri mesece. Upravljavec se odloči, da jih bo hranil v ločenih podatkovnih zbirkah v istem strežniku ter za shranjevanje uporabil pregledno šifriranje in šifriranje na ravni stolpca. Dešifrirni ključi na ravni stolpca so shranjeni v namenskih varnostnih modulih, ki jih lahko pooblaščeno osebje zgolj uporabi, ne pa izlušči.

Sistem je zaradi obvladovanja prihodnjih incidentov vzdržljivejši in zanesljivejši. Upravljavec podatkov razume, da morajo biti preventivni in učinkoviti ukrepi ter zaščitni ukrepi vgrajeni v vse sedanje in prihodnje obdelave osebnih podatkov ter da se s tem lahko pomaga preprečiti prihodnje take incidente varstva podatkov.

Upravljavec teh varnostnih ukrepov ne vzpostavi samo za zagotavljanje točnosti, celovitosti in zaupnosti, ampak tudi za preprečevanje širjenja zlonamerne programske opreme s kibernetskimi napadi in zagotovitev zanesljivosti rešitve. Zanesljivi varnostni ukrepi pripomorejo k vzpostavitvi zaupanja s posamezniki, na katere se nanašajo osebni podatki.

3.9 Odgovornost[41]

86. Načelo odgovornosti določa, da je upravljavec odgovoren za skladnost z vsemi zgoraj navedenimi načeli in jih je zmožen dokazati.

87. Upravljavec mora biti zmožen dokazati skladnost z načeli. Pri tem lahko dokaže učinke ukrepov, sprejetih za varstvo pravic posameznikov, na katere se nanašajo osebni podatki, ter zakaj se šteje, da so ukrepi ustrezni in učinkoviti. Dokaže na primer, zakaj je ukrep ustrezen za učinkovito zagotovitev načela omejitve shranjevanja.

88. Da bi lahko upravljavec osebne podatke odgovorno obdeloval, mora imeti znanje in biti zmožen izvajati varstvo podatkov. Med drugim mora svoje obveznosti glede varstva podatkov iz Splošne uredbe o varstvu podatkov razumeti ter jih biti zmožen izpolniti.

4 ČLEN 25(3) – POTRJEVANJE

89. V skladu s členom 25(3) se lahko potrjevanje v skladu s členom 42 uporabi za dokazovanje skladnosti z zahtevo vgrajenega in privzetega varstva podatkov. Nasprotno pa so lahko v postopku potrjevanja koristni tudi dokumenti, ki dokazujejo skladnost z vgrajenim in privzetim varstvom podatkov. To pomeni, da če je bilo dejanje obdelave, ki ga izvede upravljavec ali obdelovalec, potrjeno v skladu s členom 42, nadzorni organi to upoštevajo pri svoji oceni skladnosti s Splošno uredbo o varstvu podatkov, še zlasti glede na vgrajeno in privzeto varstvo podatkov.

[41] Glej uvodno izjavo 74, v skladu s katero morajo upravljavci dokazati učinkovitost svojih ukrepov.

90. Če je dejanje obdelave, ki ga izvede upravljavec ali obdelovalec, potrjeno v skladu s členom 42, so elementi, ki pripomorejo k dokazovanju skladnosti s členom 25(1) in (2), postopki oblikovanja, tj. postopek določanja sredstev obdelave, upravljanje ter tehnični in organizacijski ukrepi za izvajanje načel varstva podatkov. Merila za potrjevanje za varstvo podatkov določijo organi za potrjevanje ali lastniki sistema potrjevanja, nato pa jih odobri pristojni nadzorni organ ali Evropski odbor za varstvo podatkov. Za nadaljnje informacije o mehanizmih potrjevanja glej smernice Evropskega odbora za varstvo podatkov o certificiranju[42] in druge ustrezne smernice, ki so objavljene na njegovem spletišču.

91. Tudi če se za dejanje obdelave podeli potrdilo v skladu s členom 42, je upravljavec še vedno odgovoren za stalno spremljanje in izboljševanje skladnosti z merili vgrajenega in privzetega varstva podatkov iz člena 25.

5 IZVAJANJE ČLENA 25 IN POSLEDICE

92. Nadzorni organi lahko ocenijo skladnost s členom 25 v skladu s postopki, navedenimi v členu 58. Popravljalna pooblastila so določena v členu 58(2) in vključujejo izdajanje opozoril, opominov, odredb za ugoditev zahtevam posameznika, na katerega se nanašajo osebni podatki, omejitve ali prepoved obdelave, upravne globe itd.

93. Vgrajeno in privzeto varstvo podatkov je tudi dejavnik pri določanju ravni denarnih kazni za kršitve Splošne uredbe o varstvu podatkov, glej člen 83(4).[43, 44]

6 PRIPOROČILA

94. Čeprav obdelovalci in proizvajalci v členu 25 niso neposredno obravnavni, so tudi sami priznani kot ključni akterji, ki omogočajo vgrajeno in privzeto varstvo podatkov ter bi morali biti seznanjeni s tem, da morajo upravljavci osebne podatke obdelovati samo s sistemi in tehnologijami z vgrajenim varstvom podatkov.

95. Kadar obdelovalci in proizvajalci obdelujejo podatke v imenu upravljavcev, bi morali uporabiti svoje strokovno znanje za vzpostavitev zaupanja ter svoje stranke, vključno z MSP, usmerjati pri oblikovanju/nabavi rešitev, ki v obdelavo vključujejo varstvo podatkov. To pa pomeni, da bi se moralo z zasnovo izdelkov in storitev olajšati izpolnjevanje potreb upravljavcev.

96. Pri izvajanju člena 25 je treba upoštevati, da je glavni cilj oblikovanja *učinkovito izvajanje* načel in *zaščite* pravic posameznikov, na katere se nanašajo osebni podatki, pri ustreznih ukrepih obdelave podatkov. Da bi se olajšalo in okrepilo sprejetje vgrajenega in privzetega varstva podatkov, se upravljavcem, pa tudi proizvajalcem in obdelovalcem priporoča naslednje:
    - Upravljavci bi morali razmišljati o varstvu podatkov od *začetnih faz* načrtovanja dejanja obdelave celo pred časom določitve sredstev obdelave.

[42] Evropski odbor za varstvo podatkov. „Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe“. Različica 3.0, 4. junij 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_sl.pdf.
[43] Člen 83(2)(d) Splošne uredbe o varstvu podatkov določa, da je treba pri naložitvi glob za kršitev te uredbe ustrezno upoštevati*„stopnj[o] odgovornosti upravljavca ali obdelovalca, pri čemer se upoštevajo tehnični in organizacijski ukrepi, ki jih je sprejel v skladu s členoma 25 in 32“.*
[44] Več informacij o globah je na voljo v dokumentu Delovne skupine iz člena 29 z naslovom „Smernice o uporabi in določanju upravnih glob za namene Uredbe 2016/679“. WP 253, 3. oktober 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – ki ga je potrdil Evropski odbor za varstvo podatkov.

- Kadar ima upravljavec pooblaščeno osebo za varstvo podatkov, Evropski odbor za varstvo podatkov spodbuja dejavno sodelovanje pooblaščene osebe za varstvo podatkov pri vključitvi vgrajenega in privzetega varstva podatkov v postopke javnega naročanja in razvoja ter celoten življenjski cikel obdelave.
- Dejanje obdelave je lahko *certificirano*. Zmožnost pridobitve certifikata za dejanje obdelave pomeni za upravljavca dodano vrednost, ko pri proizvajalcih ali obdelovalcih izbira med različno programsko opremo, strojno opremo, storitvami in/ali sistemi za obdelavo. Zato bi si morali proizvajalci prizadevati, da dokažejo vgrajeno in privzeto varstvo podatkov v življenjskem ciklu njihovega razvoja rešitve za obdelavo. Certifikat lahko posameznike, na katere se nanašajo osebni podatki, tudi usmerja pri izbiri med različnim blagom in storitvami. Zmožnost pridobitve certifikata za obdelavo je lahko konkurenčna prednost za proizvajalce, obdelovalce in upravljavce ter lahko celo poveča zaupanje posameznikov, na katere se nanašajo osebni podatki, v obdelavo njihovih osebnih podatkov. Če certifikata ni, bi si morali upravljavci prizadevati za pridobitev drugih *jamstev*, da proizvajalci ali obdelovalci izpolnjujejo zahteve vgrajenega in privzetega varstva podatkov.
- Upravljavci, obdelovalci in proizvajalci bi morali upoštevati svoje obveznosti, da otrokom, mlajšim od 18 let, in drugim ranljivim skupinam zagotovijo posebno zaščito pri izpolnjevanju zahtev glede vgrajenega in privzetega varstva podatkov.
- Proizvajalci in obdelovalci bi si morali prizadevati za okrepitev izvajanja vgrajenega in privzetega varstva podatkov, da bi podprli zmožnost upravljavca za izpolnjevanje zahtev iz člena 25. Upravljavci, na drugi strani, ne bi smeli izbrati proizvajalcev ali obdelovalcev, ki ne ponujajo sistemov, ki upravljavcu omogočajo izpolnjevanje člena 25 ali ga pri tem podpirajo, ker so upravljavci odgovorni za njegovo neizvajanje.
- Proizvajalci in obdelovalci bi morali imeti dejavno vlogo pri zagotavljanju, da so izpolnjena merila „najnovejšega tehnološkega razvoja“, in obveščanju upravljavcev o kakršnih koli spremembah tega razvoja, ki lahko vplivajo na učinkovitost vzpostavljenih ukrepov. Upravljavci bi morali to zahtevo vključiti kot pogodbeno klavzulo, s čimer zagotovijo, da so seznanjeni z najnovejšo tehnologijo.
- Evropski odbor za varstvo podatkov upravljavcem priporoča, naj od proizvajalcev in obdelovalcev zahtevajo, da dokažejo, kako njihova strojna oprema, programska oprema, storitve ali sistemi upravljavcu omogočajo izpolnjevanje zahtev glede odgovornosti v skladu z vgrajenim in privzetim varstvom podatkov, na primer z uporabo ključnih kazalnikov uspešnosti za dokazovanje učinkovitosti ukrepov in zaščitnih ukrepov pri izvajanju načel in pravic.
- Evropski odbor za varstvo podatkov poudarja potrebo po usklajenem pristopu za učinkovito izvajanje načel in pravic, združenja ali organe pa spodbuja k pripravi kodeksov ravnanja v skladu s členom 40, da bi vključili tudi smernice za posamezne sektorje o vgrajenem in privzetem varstvu.
- Upravljavci bi morali posameznikom, na katere se nanašajo osebni podatki, pošteno in pregledno predstaviti, kako ocenjujejo in dokazujejo učinkovito izvajanje vgrajenega in privzetega varstva podatkov, enako kot upravljavci dokazujejo skladnost z načelom odgovornosti iz Splošne uredbe o varstvu podatkov.
- Najsodobnejše tehnologije za boljše varovanje zasebnosti se lahko uporabijo kot ukrep v skladu z zahtevami vgrajenega in privzetega varstva podatkov, če je to primerno, v okviru pristopa na podlagi tveganja. Tehnologije za boljše varovanje zasebnosti same po sebi ne zajemajo nujno obveznosti iz člena 25. Upravljavci ocenijo, ali je ukrep ustrezen in učinkovit

pri izvajanju načel varstva podatkov in pravic posameznikov, na katere se nanašajo osebni podatki.

- Za obstoječe sisteme se uporabljajo enake zahteve vgrajenega in privzetega varstva podatkov kot za nove. Če obstoječi sistemi še niso skladni z vgrajenim in privzetim varstvom podatkov in ni mogoče izvesti sprememb, na podlagi katerih bi izpolnjevali obveznosti, obstoječi sistem preprosto ne izpolnjuje obveznosti iz Splošne uredbe o varstvu podatkov in se ne more uporabljati za obdelavo osebnih podatkov.
- Člen 25 ne znižuje praga zahtev za MSP. Naslednje točke lahko olajšajo skladnost MSP s členom 25:
    - zgodnje izvajanje ocen tveganja,
    - začetek z manj obsežno obdelavo, ki se pozneje razširi in izpopolni,
    - iskanje jamstev proizvajalcev in obdelovalcev glede vgrajenega in privzetega varstva podatkov, kot je potrdilo ali upoštevanje kodeksa ravnanja,
    - sodelovanje s partnerji z dobrimi rezultati,
    - pogovor z organi za varstvo podatkov,
    - seznanitev s smernicami organov za varstvo podatkov in Evropskega odbora za varstvo podatkov,
    - upoštevanje kodeksa ravnanja, če je na voljo,
    - pridobitev strokovne pomoči in nasvetov.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)