Smjernice

Smjernice 4/2019 o članku 25.

Tehnička i integrirana zaštita podataka

Verzija 2.0

Doneseno 20. listopada 2020.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Povijest verzija

Verzija 1.0	13. studenoga 2019.	Donošenje Smjernica za javno savjetovanje
Verzija 2.0	20. listopada 2020.	Donošenje Smjernica Europskog odbora za zaštitu podataka nakon javnog savjetovanja

Sadržaj

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: Opća uredba o zaštiti podataka),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.,

uzimajući u obzir članak 12. i članak 22. svojeg Poslovnika,

DONIO JE SLJEDEĆE SMJERNICE:

Sažetak

U svijetu koji se sve više digitalizira usklađenost sa zahtjevima u pogledu tehničke i integrirane zaštite podataka ima ključnu ulogu u promicanju zaštite privatnosti i podataka u društvu. Stoga je ključno da voditelji obrade tu odgovornost ozbiljno shvate i pri izradi postupaka obrade provedu obveze iz Opće uredbe o zaštiti podataka.

U ovim se Smjernicama iznose opće preporuke o obvezi u pogledu tehničke i integrirane zaštite podataka utvrđenoj u članku 25. Opće uredbe o zaštiti podataka. Svi voditelji obrade imaju obvezu osigurati tehničku i integriranu zaštitu podataka, neovisno o veličini i razlikama u složenosti obrade. Kako bi mogao provoditi zahtjeve u pogledu tehničke i integrirane zaštite podataka, ključno je da voditelj obrade razumije načela zaštite podataka te prava i slobode ispitanika.

Temeljna je obveza provesti *odgovarajuće* mjere i potrebne zaštitne mjere kojima se osigurava *učinkovita provedba načela zaštite podataka,* a time i *tehnička i integrirana zaštita prava i sloboda ispitanika*. Člankom 25. propisuju se tehnički i integrirani elementi koji bi se trebali uzeti u obzir. Ti će se elementi dodatno razraditi u ovim Smjernicama.

U članku 25. stavku 1. navodi se da bi voditelji obrade u samom početku, pri planiranju novog postupka obrade, trebali razmotriti tehničku i integriranu zaštitu podataka. Voditelji obrade obvezni su provesti tehničku i integriranu zaštitu podataka *prije* obrade, ali i *kontinuirano* u vrijeme obrade tako da redovito preispituju učinkovitost odabranih mjera i zaštitnih mjera. Tehnička i integrirana zaštita podataka primjenjuje se i na postojeće sustave u okviru kojih se obrađuju osobni podatci.

Smjernice sadržavaju i upute za učinkovitu provedbu načela zaštite podataka iz članka 5. Opće uredbe o zaštiti podataka, a u njima su navedeni ključni elementi tehničke i integrirane zaštite podataka te ogledni primjeri iz prakse. Voditelj obrade trebao bi razmotriti jesu li mjere odgovarajuće u kontekstu konkretnog postupka obrade.

Europski odbor za zaštitu podataka iznosi preporuke o načinu na koji voditelji obrade, izvršitelji obrade i proizvođači mogu surađivati kako bi ostvarili tehničku i integriranu zaštitu podataka. Potiče voditelje obrade u industriji, izvršitelje obrade i proizvođače da primjenjuju tehničku i integriranu zaštitu podataka kako bi stvorili konkurentsku prednost pri stavljanju na tržište proizvoda namijenjenih

voditeljima obrade i ispitanicima. Isto tako, potiče sve voditelje obrade da upotrebljavaju certifikate i kodekse ponašanja.

1 PODRUČJE PRIMJENE

1. Središnja je tema ovih Smjernica način na koji voditelji obrade provode tehničku i integriranu zaštitu podataka na temelju obveze iz članka 25. Opće uredbe o zaštiti podataka.[1] Drugim subjektima, kao što su izvršitelji obrade, proizvođači proizvoda, usluga i aplikacija (dalje u tekstu: proizvođači), koji se ne spominju izravno u članku 25., ove Smjernice isto tako mogu biti korisne za stvaranje proizvoda i usluga usklađenih s Općom uredbom o zaštiti podataka, kojima se voditeljima obrade omogućuje da ispune svoje obveze u pogledu zaštite podataka.[2] U uvodnoj izjavi 78. Opće uredbe o zaštiti podataka dodaje se da bi se tehnička i integrirana zaštita podataka trebala uzeti u obzir u kontekstu javnih natječaja. Unatoč tome što su svi voditelji obrade dužni uključiti tehničku i integriranu zaštitu podataka u svoje aktivnosti obrade, tom se odredbom potiče usvajanje načela zaštite podataka, pri čemu bi javna uprava trebala služiti kao primjer. Voditelji obrade odgovorni su za ispunjenje obveza u pogledu tehničke i integrirane zaštite podataka pri obradi koju provode njihovi izvršitelji i podizvršitelji obrade. Stoga bi voditelji obrade to trebali uzeti u obzir pri sklapanju ugovora s tim stranama.

2. U skladu sa zahtjevom opisanim u članku 25., voditelji obrade moraju uključiti elemente tehničke i integrirane zaštite podataka u obradu osobnih podataka, a to se primjenjuje tijekom cijelog životnog ciklusa obrade. Zahtjev u pogledu tehničke i integrirane zaštite podataka odnosi se i na sustave za obradu koji su postojali prije nego što je Opća uredba o zaštiti podataka stupila na snagu. Voditelji obrade moraju redovito ažurirati postupak obrade u skladu s Općom uredbom o zaštiti podataka. Za dodatne informacije o održavanju postojećeg sustava u skladu s tehničkom i integriranom zaštitom podataka vidjeti potpoglavlje 2.1.4. ovih Smjernica. Tom se odredbom ponajprije želi zajamčiti *primjerena* i *učinkovita* zaštita podataka, uz poštovanje njezinih *tehničkih* i *integriranih* elemenata, što znači da bi voditelji obrade trebali moći dokazati da imaju uspostavljene odgovarajuće mjere i zaštitne mjere kako bi osigurali da su načela zaštite podataka te prava i slobode ispitanika učinkoviti.

3. Drugo poglavlje Smjernica usmjereno je na tumačenje zahtjevâ navedenih u članku 25. te se u njemu istražuju pravne obveze uvedene tom odredbom. Primjeri primjene tehničke i integrirane zaštite podataka u kontekstu posebnih načela zaštite podataka navedeni su u trećem poglavlju.

4. U četvrtom poglavlju Smjernica razmatra se mogućnost uspostave mehanizma certificiranja za dokazivanje usklađenosti s člankom 25., a u petom poglavlju način na koji nadzorna tijela mogu primjenjivati taj članak. Naposljetku, u Smjernicama se dionicima iznose dodatne preporuke o tome kako uspješno provesti tehničku i integriranu zaštitu podataka. Europski odbor za zaštitu podataka prepoznaje izazove s kojima se suočavaju mala i srednja poduzeća (dalje u tekstu: MSP-ovi) dok nastoje u potpunosti ispuniti obveze u pogledu tehničke i integrirane zaštite podataka, a u šestom poglavlju daje dodatne preporuke koje se posebno odnose na MSP-ove.

[1] Navedena tumačenja jednako su primjenjiva na članak 20. Direktive (EU) 2016/680 i članak 27. Uredbe (EU) 2018/1725.

[2] U uvodnoj izjavi 78. Opće uredbe o zaštiti podataka jasno se navodi ta potreba: „Prilikom razvijanja, osmišljavanja, odabira i upotrebe aplikacija, usluga i proizvoda koji se temelje na obradi osobnih podataka ili obrađuju osobne podatke kako bi ispunili svoju zadaću, proizvođače proizvoda, usluga i aplikacija trebalo bi poticati da uzmu u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija i da uzimajući u obzir najnovija dostignuća osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka.”

2 ANALIZA TEHNIČKE I INTEGRIRANE ZAŠTITE PODATAKA IZ ČLANKA 25. STAVAKA 1. I 2.

5. Svrha je ovog poglavlja istražiti zahtjeve za tehničku zaštitu podataka iz članka 25. stavka 1. i za integriranu zaštitu podataka iz članka 25. stavka 2. Opće uredbe o zaštiti podataka te dati smjernice o tim zahtjevima. Tehnička i integrirana zaštita podataka povezani su koncepti koji se međusobno nadopunjuju. Ispitanici će imati veću korist od integrirane zaštita podataka ako se istodobno s njom provodi tehnička zaštita podataka, i obratno.

6. Tehnička i integrirana zaštita podataka obvezna je za sve voditelje obrade, uključujući mala i multinacionalna poduzeća. S obzirom na to, složenost provedbe tehničke i integrirane zaštite podataka može se razlikovati ovisno o pojedinačnom postupku obrade. Ipak, neovisno o veličini, voditelj obrade i ispitanik u svim slučajevima mogu ostvariti koristi od provedbe tehničke i integrirane zaštite podataka.

2.1 Članak 25. stavak 1.: Tehnička zaštita podataka

2.1.1 Obveza voditelja obrade da provede odgovarajuće tehničke i organizacijske mjere te potrebne zaštitne mjere u vezi s obradom

7. U skladu s člankom 25. stavkom 1. voditelj obrade provodi *odgovarajuće* tehničke i organizacijske *mjere* koje su osmišljene radi provedbe načela zaštite podataka i integracije *potrebnih zaštitnih mjera* u obradu kako bi se ispunili zahtjevi te zaštitila prava i slobode ispitanika. Odgovarajuće mjere i potrebne zaštitne mjere trebale bi služiti istoj svrsi zaštite pravâ ispitanika i osigurati da je zaštita njihovih osobnih podataka uvrštena u obradu.

8. Pojmovi *tehničke i organizacijske mjere* i potrebne *zaštitne mjere* mogu se tumačiti u širem smislu kao bilo koja metoda ili način koje voditelj obrade može upotrebljavati pri obradi. Pojam *odgovarajuće* znači da bi mjere i potrebne zaštitne mjere trebale biti prikladne za postizanje predviđene svrhe, odnosno njima se mora provoditi *učinkovita*[3] zaštita podataka. Zahtjev da mjere budu odgovarajuće stoga je usko povezan sa zahtjevom učinkovitosti.

9. Tehničke ili organizacijske mjere te zaštitne mjere mogu se odnositi na npr. napredna tehnička rješenja i osnovno osposobljavanje osoblja. Primjeri koji mogu biti prikladni, ovisno o kontekstu i rizicima povezanima s predmetnom obradom, uključuju pseudonimizaciju osobnih podataka[4], pohranu dostupnih osobnih podataka u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, omogućavanje ispitanicima da utječu na obradu, pružanje informacija o pohrani osobnih podataka, uspostavu sustava za detekciju zlonamjernog softvera, osposobljavanje zaposlenika o osnovnoj „kiberhigijeni", utvrđivanje sustava za upravljanje privatnošću i sigurnošću informacija, ugovorno obvezivanje izvršitelja obrade na provedbu konkretnih praksi smanjenja količine podataka itd.

10. Za utvrđivanje odgovarajućih mjera mogu biti korisni standardi, najbolja praksa i kodeksi ponašanja koje su priznala udruženja i druga tijela koja predstavljaju kategorije voditelja obrade. Međutim, voditelj obrade mora provjeriti jesu li mjere odgovarajuće za predmetnu obradu.

[3] „Učinkovitost" se pomnije obrađuje u nastavku u potpoglavlju 2.1.2.
[4] Definirano u članku 4. stavku 5. Opće uredbe o zaštiti podataka.

2.1.2 Osmišljeno za učinkovitu provedbu načela zaštite podataka i zaštitu prava i sloboda ispitanika

11. *Načela zaštite podataka* navedena su u članku 5. (dalje u tekstu: načela). *Prava i slobode ispitanika* temeljna su prava i slobode pojedinaca, posebno njihovo pravo na zaštitu osobnih podataka, a ta se zaštita u članku 1. stavku 2. navodi kao cilj Opće uredbe o zaštiti podataka (dalje u tekstu: prava)[5]. Ta su prava preciznije formulirana u Povelji EU-a o temeljnim pravima. Iznimno je važno da voditelj obrade razumije značenje *načela* i *prava* kao osnova za zaštitu koja se jamči Općom uredbom o zaštiti podataka, konkretno obvezom u pogledu tehničke i integrirane zaštite podataka.

12. Pri provedbi odgovarajućih tehničkih i organizacijskih mjera te mjere i zaštitne mjere trebale bi biti *osmišljene* kako bi se osigurale učinkovita provedba svakog prethodno navedenog načela i zaštita prava koja iz toga proizlaze.

Rješavanje pitanja učinkovitosti

13. Učinkovitost je u središtu koncepta tehničke zaštite podataka. Zahtjev za učinkovitu provedbu načelâ podrazumijeva da voditelji obrade moraju provesti potrebne mjere i zaštitne mjere kako bi zaštitili ta načela i u konačnici zajamčili prava ispitanika. Svakom provedenom mjerom trebao bi se u okviru obrade postići rezultat koji je voditelj obrade želio ostvariti. Ovo zapažanje ima dvije posljedice.

14. Prvo, to znači da se člankom 25. ne zahtijeva provedba posebnih tehničkih i organizacijskih mjera, nego da bi odabrane mjere i zaštitne mjere trebale biti prilagođene provedbi načelâ zaštite podataka u okviru predmetne obrade. Te bi mjere i zaštitne mjere pritom trebale biti osmišljene tako da budu dovoljno opsežne, a voditelj obrade trebao bi moći provesti dodatne mjere kako bi se prilagodio mogućem povećanju rizika[6]. Stoga će učinkovitost mjera ovisiti o kontekstu predmetne obrade i procjeni određenih elemenata koji bi se trebali uzeti u obzir pri utvrđivanju načina obrade. Prethodno navedeni elementi detaljnije će se obraditi u potpoglavlju 2.1.3. u nastavku.

15. Drugo, voditelji obrade trebali bi moći dokazati da su načela očuvana.

16. Provedenim mjerama i zaštitnim mjerama trebao bi se postići željeni učinak u pogledu zaštite podataka, a voditelj obrade trebao bi imati dokumentaciju o provedenim tehničkim i organizacijskim mjerama[7]. U tu svrhu voditelj obrade može utvrditi odgovarajuće ključne pokazatelje uspješnosti za dokazivanje učinkovitosti. Ključni pokazatelj uspješnosti mjerljiva je vrijednost koju odabire voditelj obrade i kojom se dokazuje koliko učinkovito voditelj obrade postiže svoj cilj zaštite podataka. Ključni pokazatelji uspješnosti mogu biti *kvantitativni*, kao što su postotak lažno pozitivnih ili lažno negativnih rezultata, smanjenje broja pritužbi i, smanjenje vremena odgovora kad ispitanici ostvaruju svoja prava, ili *kvalitativni*, kao što su evaluacije uspješnosti, uporaba ljestvice za razvrstavanje ili stručne procjene. Umjesto s pomoću ključnih pokazatelja uspješnosti voditelji obrade mogu dokazati učinkovitost provedbe načela tako da iznesu obrazloženje svoje procjene učinkovitosti odabranih mjera i zaštitnih mjera.

[5] Vidjeti uvodnu izjavu 4. Opće uredbe o zaštiti podataka.

[6] „Temeljna načela koja su primjenjiva na voditelje obrade (tj. legitimnost, ograničavanje količine podataka, ograničavanje svrhe, transparentnost, cjelovitost podataka, točnost podataka) trebaju ostati ista, bez obzira na obradu i rizike za ispitanike. Međutim, uzimanje u obzir prirode i opsega takve obrade uvijek je bilo sastavni dio primjene tih načela, tako da su ona sama po sebi prilagodljiva." Radna skupina iz članka 29. „Izjava o ulozi pristupa temeljenog na riziku u pravnim okvirima za zaštitu podataka". WP 218, 30. svibnja 2014., str. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Vidjeti uvodne izjave 74. i 78.

2.1.3 Elementi koje treba uzeti u obzir

17. U članku 25. stavku 1. navedeni su elementi koje voditelj obrade mora uzeti u obzir pri određivanju mjera određenog postupka obrade. U nastavku ćemo iznijeti upute o primjeni tih elemenata tijekom postupka osmišljavanja, kojim je obuhvaćena i izrada integriranih postavki. Svi ti elementi pomažu pri utvrđivanju je li određena mjera odgovarajuća za učinkovitu provedbu načela. Stoga svaki od tih elemenata nije cilj sam po sebi, već je riječ o čimbenicima koje treba uzeti u obzir zajedno kako bi se ostvario određeni cilj.

2.1.3.1 „Najnovija dostignuća"

18. Koncept „najnovijih dostignuća" prisutan je u različitim pravnim stečevinama EU-a, npr. zaštiti okoliša i sigurnosti proizvoda. U Općoj uredbi o zaštiti podataka upućivanje na „najnovija dostignuća"[8] javlja se u članku 32. za sigurnosne mjere[9][10], ali i u članku 25., čime se ta referentna vrijednost proširuje na sve tehničke i organizacijske mjere uvrštene u obradu.

19. U kontekstu članka 25., upućivanje na „najnovija dostignuća" voditelje obrade obvezuje da pri utvrđivanju odgovarajućih tehničkih i organizacijskih mjera **uzmu u obzir postojeći napredak tehnologije** koji je dostupan na tržištu. Taj zahtjev podrazumijeva da voditelji obrade moraju biti upoznati i u tijeku s tehnološkim napretkom, načinima na koje tehnologija može biti povezana s rizicima u području zaštite podataka ili mogućnostima u postupku obrade te načinima na koje se mogu provesti i ažurirati mjere i zaštitne mjere kojima se *osigurava učinkovita provedba* načela i prava ispitanika s obzirom na promjenjivo tehnološko okružje.

20. „Najnovija dostignuća" dinamičan je pojam koji se ne može statički definirati u određenom trenutku, već bi ga trebalo *stalno* ocjenjivati u kontekstu tehnološkog napretka. S obzirom na tehnološki napredak, voditelj obrade mogao bi ustanoviti da mjera koja je nekada pružala odgovarajuću razinu zaštite sada to više ne čini. Propusti li se ostati u korak s tehnološkim promjenama, to bi moglo dovesti do neusklađenosti s člankom 25.

21. Kriterij „najnovijeg dostignuća" ne primjenjuje se samo na tehnološke, nego i na organizacijske mjere. Nedostatak odgovarajućih organizacijskih mjera može smanjiti ili čak u potpunosti ugroziti učinkovitost odabrane tehnologije. Primjeri organizacijskih mjera mogu biti donošenje internih politika, suvremeno osposobljavanje o tehnologiji, sigurnosti i zaštiti podataka te politike za upravljanje sigurnošću informacijske tehnologije.

22. Postojeći i potvrđeni okviri, standardi, certifikacije, kodeksi ponašanja itd. u različitim područjima mogu biti važan pokazatelj najnovijih dostignuća u određenom području primjene. Ako takvi standardi postoje i ako se njima pruža visoka razina zaštite ispitanika koja je u skladu s pravnim zahtjevima, ili pak prelazi te zahtjeve, voditelji obrade trebali bi ih uzeti u obzir pri osmišljavanju i provedbi mjera za zaštitu podataka.

---

[8] Vidjeti odluku njemačkog Saveznog ustavnog suda „Kalkar" iz 1978.: https://germanlawarchive.iuscomp.org/?p=67, koja može postaviti temelje za metodologiju objektivne definicije koncepta. Na temelju toga, „najnovija dostignuća" u tehnologiji utvrđivala bi se između „postojećih znanstvenih spoznaja i istraživačkih" tehnoloških razina te utvrđenijih „općeprihvaćenih pravila tehnologije." „Najnovija dostignuća" stoga se može prepoznati kao tehnološki stupanj usluge ili tehnologije ili proizvoda koji postoji na tržištu, a najučinkovitiji je u postizanju utvrđenih ciljeva.

[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/

2.1.3.2 „Trošak provedbe”

23. Pri odabiru i primjeni odgovarajućih tehničkih i organizacijskih mjera te potrebnih zaštitnih mjera kojima se učinkovito provode načela kako bi se zaštitila prava ispitanika, voditelj obrade može u obzir uzeti trošak provedbe. Trošak se odnosi na sredstva općenito, uključujući vrijeme i ljudske resurse.

24. Element troška ne podrazumijeva da voditelj obrade mora potrošiti nerazmjernu količinu resursa ako postoje alternativne, a opet učinkovite, mjere za čiju je provedbu potrebna manja količina resursa. Ipak, trošak provedbe čimbenik je koji bi se trebao uzeti u obzir pri provedbi tehničke zaštite podataka, ali ne bi smio biti razlogom za odustajanje od njezine provedbe.

25. Stoga se odabranim mjerama mora osigurati da se u okviru aktivnosti obrade koje je predvidio voditelj obrade osobni podatci ne obrađuju protivno načelima, neovisno o trošku. Voditelji obrade trebali bi moći upravljati ukupnim troškom kako bi mogli učinkovito provesti sva načela i na taj način zaštititi prava.

2.1.3.3 „Priroda, opseg, kontekst i svrha obrade”

26. Pri utvrđivanju potrebnih mjera voditelji obrade moraju u obzir uzeti prirodu, opseg, kontekst i svrhu obrade.

27. Ti bi se čimbenici trebali tumačiti u skladu s njihovom ulogom u drugim odredbama Opće uredbe o zaštiti podataka, kao što su članci 24., 32. i 35., kako bi se u obradu uključila načela zaštite podataka.

28. Ukratko, pojam **priorode** može se shvatiti kao inherentna[11] značajka obrade. **Opseg** se odnosi na veličinu i raspon obrade. **Kontekst** se odnosi na okolnosti obrade, koje mogu utjecati na očekivanja ispitanika, dok se **svrha** odnosi na ciljeve obrade.

2.1.3.4 „Rizici različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka”

29. U brojnim odredbama Opće uredbe o zaštiti podataka, konkretno u člancima 24., 25., 32. i 35., primjenjuje se dosljedan pristup temeljen na riziku u cilju utvrđivanja odgovarajućih tehničkih i organizacijskih mjera za zaštitu pojedinaca, njihovih osobnih podataka i ispunjavanje zahtjeva Opće uredbe o zaštiti podataka. Predmet zaštite uvijek je isti (pojedinci čiji se osobni podatci nastoje zaštiti), zaštita koja se osigurava odnosi se na iste rizike (one za prava pojedinaca) i pritom se u obzir uzimaju isti uvjeti (priroda, opseg, kontekst i svrhe obrade).

30. Pri provedbi analize rizika radi usklađenosti s člankom 25. voditelj obrade mora utvrditi rizike za prava ispitanika koji nastaju zbog povrede načela te odrediti razinu vjerojatnosti i ozbiljnosti kako bi proveo mjere za učinkovito ublažavanje utvrđenih rizika. Tijekom procjena rizika ključno je provesti sustavnu i temeljitu evaluaciju obrade. Na primjer, voditelj obrade procjenjuje određene rizike povezane s nedostatkom dobrovoljno dane privole, što čini povredu načela zakonitosti, tijekom obrade osobnih podataka djece i osoba mlađih od 18 godina kao ranjive skupine, ako ne postoje druge pravne osnove, te provodi odgovarajuće mjere kako bi odgovorio na utvrđene rizike povezane s tom skupinom ispitanika i učinkovito ih ublažio.

[11] Primjeri su posebne kategorije osobnih podataka, automatsko odlučivanje, iskrivljeni odnosi moći, nepredvidljiva obrada, poteškoće ispitanika pri ostvarivanju prava itd.

31. U Smjernicama Europskog odbora za zaštitu podataka o procjeni učinka na zaštitu podataka[12], čija je središnja tema utvrđivanje vjerojatnosti da će postupak obrade prouzročiti visok rizik za ispitanika, daju se i upute za procjenu rizika za zaštitu podataka i provedbu procjene rizika za zaštitu podataka. Te smjernice mogu biti korisne i tijekom procjene rizika u svim prethodno navedenim člancima, uključujući članak 25.

32. Pristup utemeljen na riziku ne isključuje primjenu osnovnih scenarija, najbolje prakse i standarda. Oni bi mogli biti koristan alat za voditelje obrade za rješavanje sličnih rizika u sličnim situacijama (priroda, opseg, kontekst i svrha obrade). Međutim, i dalje se mora ispunjavati obveza iz članka 25. (te članaka 24. i 32. i članka 35. stavka 7. točke (c)) da se u obzir uzimaju „rizici različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka". Stoga voditelji obrade, iako na raspolaganju imaju takve alate, uvijek moraju za svaku pojedinu aktivnost obrade podataka provesti procjenu rizika za zaštitu podataka i provjeriti učinkovitost predloženih odgovarajućih mjera i zaštitnih mjera. Usto bi mogle biti potrebne Smjernice o procjeni učinka na zaštitu podataka ili ažurirana verzija tih smjernica.

2.1.4 Vremenski aspekt

2.1.4.1 U vrijeme određivanja sredstava obrade

33. Tehnička zaštita podataka provodi se „u vrijeme određivanja sredstava obrade".

34. „Sredstva obrade" mogu biti općeniti i detaljni tehnički elementi obrade, kao što su arhitektura, postupci, protokoli, raspored i izgled.

35. „Vrijeme određivanja sredstava obrade" odnosi se na vremensko razdoblje u kojem voditelj obrade odlučuje o načinu na koji će provesti obrada podataka, načinu na koji će se ta obrada odvijati i mehanizmima koji će se upotrijebiti za njezinu provedbu. U postupku donošenja takvih odluka voditelj obrade mora procijeniti odgovarajuće mjere i zaštitne mjere za učinkovitu provedbu načela i zaštitu prava ispitanika u okviru obrade te uzeti u obzir elemente kao što su najnovija dostignuća, troškovi provedbe, priroda, opseg, kontekst i svrha obrade te rizici. To uključuje vrijeme nabave i uvođenja softvera, hardvera i usluga za potrebe obrade podataka.

36. Rano razmatranje tehničke i integrirane zaštite podataka ključno je za uspješnu provedbu načela i zaštitu prava ispitanika. Osim toga, kad je riječ o troškovima i koristi, u najboljem je interesu voditelja obrade da što prije razmotri tehničku i integriranu zaštitu podataka jer postupak naknadne promjene planova koji su već izrađeni i postupaka obrade koji su već osmišljeni može biti zahtjevan i skup.

2.1.4.2 U vrijeme same obrade (održavanje i preispitivanje zahtjeva za zaštitu podataka)

37. Nakon što obrada započne, voditelj obrade obvezan je kontinuirano održavati tehničku i integriranu zaštitu podataka, odnosno kontinuirano i učinkovito provoditi načela kako bi zaštitio prava, biti u tijeku s najnovijim dostignućima, ponovno procijeniti razinu rizika itd. Priroda, opseg i kontekst postupaka obrade, kao i rizik, mogu se tijekom obrade promijeniti, što znači da voditelj obrade mora ponovno ocijeniti svoje postupke obrade tako što će provoditi redovita preispitivanja i procjene učinkovitosti mjera i zaštitnih mjera koje je odabrao.

[12] „Smjernice o procjeni učinka na zaštitu podataka" i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe (EU) 2016/679, koje je donijela radna skupina iz članka 29. WP 248 rev.01, 4. listopada 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – potvrdio Europski odbor za zaštitu podataka

38. Obveza održavanja, preispitivanja i ažuriranja postupka obrade, prema potrebi, primjenjuje se i na postojeće sustave. To znači da se naslijeđeni sustavi koji su izrađeni prije nego što je Opća uredba o zaštiti podataka stupila na snagu moraju preispitivati i održavati kako bi se osigurala provedba mjera i zaštitnih mjera kojima se učinkovito provode načela i štite prava ispitanika, kako je navedeno u ovim Smjernicama.

39. Tom je obvezom obuhvaćena i svaka obrada koju provode izvršitelji obrade podataka. Voditelji obrade trebali bi redovito preispitivati i procjenjivati postupke izvršitelja obrade kako bi se zajamčilo da su ti postupci u svakom trenutku usklađeni s načelima i kako bi se u okviru njih voditeljima obrade omogućilo da ispune svoje obveze u tom pogledu.

2.2 Članak 25. stavak 2.: Integrirana zaštita podataka

2.2.1 Integriranim načinom obrađuju se samo osobni podatci koji su nužni za svaku posebnu svrhu obrade.

40. „Integrirano", kako je uobičajeno definirano u računalstvu, odnosi se na postojeću ili prethodno odabranu vrijednost koja se može konfigurirati, a koja se dodjeljuje nekoj softverskoj aplikaciji, računalnom programu ili uređaju. Te se postavke nazivaju i „zadane postavke" ili „tvorničke postavke", posebno kada je riječ o elektroničkim uređajima.

41. Stoga se pojam „integrirano" u kontekstu obrade osobnih podataka odnosi na donošenje odluka o vrijednostima konfiguracije ili mogućnostima obrade koje su dodijeljene ili propisane u okviru sustava za obradu, kao što je softverska aplikacija, usluga ili uređaj ili postupak ručne obrade koji utječu na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje njihove pohrane i njihovu dostupnost.

42. Voditelj obrade trebao bi odabrati integrirane postavke i mogućnosti obrade te biti odgovoran za njihovu provedbu tako da osigura da se integriranim načinom provodi samo obrada koja je izričito nužna za ispunjenje utvrđene zakonite svrhe. Pri tome bi se voditelji obrade trebali osloniti na vlastitu procjenu nužnosti obrade s obzirom na pravnu osnovu iz članka 6. stavka 1. To znači da integriranim načinom voditelj obrade prikuplja samo nužnu količinu podataka, obrađuje prikupljene podatke samo za nužne svrhe i pohranjuje te podatke samo na nužno razdoblje. Osnovni je zahtjev da zaštita podataka bude integrirani element obrade.

43. Od voditelja obrade zahtijeva se da unaprijed odredi za koje se određene, izričite i zakonite svrhe osobni podatci prikupljaju i obrađuju[13]. Mjere same po sebi moraju biti primjerene kako bi se osiguralo da se obrađuju samo osobni podatci koji su potrebni za svaku određenu svrhu obrade. Smjernice Europskog nadzornika za zaštitu podataka za procjenu nužnosti i proporcionalnosti mjera kojima se ograničava pravo na zaštitu osobnih podataka mogu biti korisne i za odlučivanje o tome koji su podatci potrebni za obradu kako bi se postigla određena svrha[14] [15] [16].

[13] Članak 5. stavak 1. točke (b), (c), (d) i (e) Opće uredbe o zaštiti podataka.
[14] EDPS. „Smjernice o procjeni nužnosti i proporcionalnosti mjera kojima se ograničava pravo na zaštitu podataka". 25. veljače 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Vidjeti i EDPS. „Procjena nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka: komplet alata" https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] Za više informacija o nužnosti vidjeti: Radna skupina iz članka 29. „Mišljenje 06/2014 o pojmu zakonitih interesa nadzornika podataka u skladu s člankom 7. Direktive 95/46/EZ". WP 217, 9. travnja 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hr.pdf

44. Ako voditelj obrade upotrebljava softver treće strane ili gotov softver, voditelj obrade trebao bi provesti procjenu rizika za proizvod i osigurati da se isključe funkcije koje nemaju pravnu osnovu ili nisu usklađene s predviđenim svrhama obrade.

45. Ista se razmatranja primjenjuju na organizacijske mjere kojima se podupiru postupci obrade. One bi trebale biti osmišljene tako da se na početku obrađuje samo minimalna količina osobnih podataka potrebnih za određene operacije. To bi se posebno trebalo uzeti u obzir pri dodjeli pristupa podatcima osoblju s različitim ulogama i različitim potrebama u pogledu pristupa.

46. Stoga se odgovarajuće „tehničke i organizacijske mjere" u kontekstu integrirane zaštite podataka tumače na isti način kako je navedeno u prethodnom potpoglavlju 2.1.1., ali se konkretno primjenjuju na provedbu načela smanjenja količine podataka.

47. Prethodno navedena obveza obrade samo onih osobnih podataka koji su potrebni za svaku određenu svrhu primjenjuje se na elemente navedene u nastavku.

2.2.2 Dimenzije obveze smanjenja količine podataka

48. U članku 25. stavku 2. navode se dimenzije obveze smanjenja količine podataka za integriranu obradu tako što se utvrđuje da se ta obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje njihove pohrane i njihovu dostupnost.

2.2.2.1 „Količina prikupljenih osobnih podataka"

49. Voditelji obrade trebali bi razmotriti i količinu osobnih podataka, kao i vrstu, kategorije i razinu detalja osobnih podataka koji su potrebni za obradu. Pri odabiru tehničkih elemenata trebali bi se uzeti u obzir veći rizici za načela cjelovitosti i povjerljivosti, smanjenje količine podataka i ograničenje pohrane pri prikupljanju velikih količina detaljnih osobnih podataka koji će se zatim usporediti s manjim rizicima u slučaju prikupljanja manjih količina i/ili manje detaljnih podataka o ispitanicima. U svakom slučaju, zadana postavka ne smije uključivati prikupljanje osobnih podataka koji nisu potrebni za određenu svrhu obrade. Drugim riječima, ako su određene kategorije osobnih podataka nepotrebne ili ako detaljni podatci nisu potrebni jer su manje granularni podatci dovoljni, tada se neće prikupljati nikakvi viškovi osobnih podataka.

50. Isti zahtjevi u pogledu integriranih postavki primjenjuju se i na usluge, neovisno o platformi ili uređaju koji se upotrebljava. Mogu se prikupljati samo osobni podatci nužni za navedenu svrhu.

2.2.2.2 „Opseg njihove obrade"

51. Postupci obrade[17] osobnih podataka ograničeni su na ono što je potrebno. Mnogi postupci obrade mogu pridonijeti svrsi obrade. Ipak, iako su određeni osobni podatci nužni kako bi se ispunila određena svrha, to ne znači da se za te podatke mogu provesti postupci obrade svih vrsta i učestalosti. Voditelji obrade trebali bi pripaziti i na to da ne prošire granice „usklađenih svrha" iz članka 6. stavka 4. i da vode računa o tome koja će vrsta obrade biti u skladu s razumnim očekivanjima ispitanika.

[17] U skladu s člankom 4. stavkom 2. Opće uredbe o zaštiti podataka to uključuje prikupljanje, bilježenje, organizaciju, strukturiranje, pohranu, prilagodbu ili izmjenu, pronalaženje, obavljanje uvida, uporabu, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

2.2.2.3 „Razdoblje pohrane”

52. Prikupljeni osobni podatci ne smiju se pohranjivati ako to nije potrebno za obradu te ako ne postoje druga usklađena svrha i pravna osnova u skladu s člankom 6. stavkom 4. Prema potrebi, svako zadržavanje podataka voditelj obrade trebao bi objektivno obrazložiti u skladu s načelom odgovornosti.

53. Voditelj obrade ograničava razdoblje zadržavanja na ono što je nužno za određenu svrhu. Ako osobni podatci više nisu potrebni za obradu, automatski se brišu ili anonimiziraju. Duljina razdoblja zadržavanja stoga će ovisiti o svrsi predmetne obrade. Ta se obveza izravno odnosi na načelo ograničenja pohrane iz članka 5. stavka 1. točke (e) i primjenjuje se automatski, odnosno voditelj obrade trebao bi imati uspostavljene sustavne postupke za brisanje ili anonimizaciju podataka obuhvaćenih obradom.

54. Anonimizacija[18] osobnih podataka alternativa je brisanju, pod uvjetom da se svi relevantni kontekstualni elementi uzmu u obzir te da se redovito procjenjuje vjerojatnost i ozbiljnost rizika, uključujući rizik od ponovnog utvrđivanja identiteta[19].

2.2.2.4 „Njihova dostupnost”

55. Voditelj obrade trebao bi na temelju procjene nužnosti ograničiti tko ima pristup osobnim podatcima i vrste pristupa koje ima te osigurati da su osobni podatci doista dostupni osobama kojima su potrebni, na primjer, u kritičnim situacijama. Načela kontrole pristupa trebala bi se poštovati za čitav protok podataka tijekom obrade.

56. U članku 25. stavku 2. osim toga se navodi da osobni podatci ne smiju biti dostupni, bez intervencije pojedinca, neograničenom broju fizičkih osoba. U skladu s integriranim pravilima voditelj obrade ograničava dostupnost i omogućuje ispitaniku da intervenira prije nego što objavi ili na drugi način na raspolaganje stavi neograničenom broju fizičkih osoba osobne podatke o ispitaniku na kojeg se podatci odnose.

57. Stavljanje na raspolaganje osobnih podataka neograničenom broju fizičkih osoba može dovesti do širenja podataka u mjeri većoj nego što se isprva planiralo. To je posebno relevantno u kontekstu interneta i tražilica. To znači da bi voditelji obrade u skladu s integriranim pravilima trebali ispitanicima dati priliku da interveniraju prije nego što se osobni podatci objave na otvorenom internetu. To je posebno važno kad je riječ o djeci i ranjivim skupinama.

58. Ovisno o pravnim osnovama za obradu, prilika za intervenciju može se razlikovati ovisno o kontekstu obrade. Na primjer, može se zatražiti privola ispitanika za javnu objavu osobnih podataka ili se mogu odrediti postavke privatnosti kako bi ispitanici sami mogli upravljati javnim pristupom.

[18] Radna skupina iz članka 29. „Mišljenje 05/2014 o tehnikama anonimizacije”. WP 216, 10. travnja 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hr.pdf

[19] Vidjeti članak 4. stavak 1. Opće uredbe o zaštiti podataka, uvodnu izjavu 26. Opće uredbe o zaštiti podataka i dokument Radne skupine iz članka 29. „Mišljenje 05/2014 o tehnikama anonimizacije”. Vidjeti i pododjeljak o „ograničenju pohrane” u odjeljku 3. ovog dokumenta, koji se odnosi na potrebu da voditelj obrade zajamči učinkovitost primijenjene tehnike odnosno tehnikâ anonimizacije.

59. Čak i u slučaju da su osobni podatci javno dostupni uz dopuštenje i razumijevanje ispitanika, to ne znači da bilo koji drugi voditelji obrade koji imaju pristup tim osobnim podatcima mogu sami, za vlastite potrebe, obraditi te podatke – oni moraju imati odvojenu pravnu osnovu[20].

3 PROVEDBA NAČELA ZAŠTITE PODATAKA PRI OBRADI OSOBNIH PODATAKA UPORABOM TEHNIČKE I INTEGRIRANE ZAŠTITE PODATAKA

60. U svim fazama osmišljavanja aktivnosti obrade, uključujući javnu nabavu, javne natječaje, eksternalizaciju, razvoj, podršku, održavanje, ispitivanje, pohranu, brisanje itd. voditelj obrade trebao bi uzeti u obzir i razmotriti različite elemente tehničke i integrirane zaštite podataka, koji će se u ovom poglavlju prikazati na primjerima u kontekstu provedbe načela[21] [22] [23].

61. Voditelji obrade trebaju provesti određena načela kako bi se osigurala tehnička i integrirana zaštita podataka. Ta su načela transparentnost, zakonitost, poštenost, ograničavanje svrhe, smanjenje količine podataka, točnost, ograničenje pohrane, cjelovitost i povjerljivost te odgovornost. Navedena su u članku 5. i uvodnoj izjavi 39. Opće uredbe o zaštiti podataka. Kako bi se u potpunosti razumio način na koji će se provesti tehnička i integrirana zaštita podataka, ističe se važnost razumijevanja značenja svakog od tih načela.

62. Pri iznošenju primjera načina na koje se može provoditi tehnička i integrirana zaštita podataka, sastavili smo popis **ključnih elemenata tehničke i integrirane zaštite podataka** za svako od tih načela. Primjerima se objašnjava određeno načelo zaštite podataka, no mogu se i preklapati s drugim usko povezanim načelima. Europski odbor za zaštitu podataka naglašava da ključni elementi i primjeri navedeni u nastavku nisu iscrpni ni obvezujući, ali bi trebali služiti kao smjernice za svako od tih načela. Voditelji obrade trebaju procijeniti na koji će način zajamčiti usklađenost s načelima u kontekstu konkretnog postupka obrade.

63. Iako je ovaj odjeljak usmjeren na provedbu načela, voditelj obrade trebao bi provesti i *odgovarajuće* i *učinkovite* načine za zaštitu prava ispitanika, isto tako i u skladu s poglavljem III. Opće uredbe o zaštiti podataka, ako se to već ne zahtijeva u okviru samih načela.

64. Načelo je odgovornosti sveobuhvatno: njime se od voditelja obrade zahtijeva da bude odgovoran pri odabiru potrebnih tehničkih i organizacijskih mjera.

3.1 Transparentnost[24]

65. Voditelj obrade mora ispitanika jasno i otvoreno obavijestiti o tome kako će prikupljati, upotrebljavati i dijeliti osobne podatke. Transparentnost će ispitanicima omogućiti da razumiju i, ako je to potrebno,

[20] Vidjeti predmet Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske br. 931/13.
[21] Više primjera može se pronaći kod norveškog tijela za zaštitu podataka. „Razvoj softvera s tehničkom i integriranom zaštitom podataka". 28. studenoga 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
[24] Razradu o tome kako razumjeti koncept transparentnosti može se pronaći u dokumentu Radne skupine iz članka 29. „Smjernice o transparentnosti na temelju Uredbe 2016/679". WP 260 rev.01, 11. travnja 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – potvrdio Europski odbor za zaštitu podataka

iskoriste svoja prava iz članaka od 15. do 22. To je načelo obuhvaćeno člancima 12., 13., 14. i 34. Mjerama i zaštitnim mjerama uspostavljenima kako bi se podržalo načelo transparentnosti trebalo bi podupirati i provedbu tih članaka.

66. Ključni tehnički i integrirani elementi transparentnosti mogu biti sljedeći:

- Jasnoća – informacije moraju biti jasne i jednostavno sročene, kratke i razumljive.
- Semantika – priopćenje bi za predmetnu publiku trebalo imati jasno značenje.
- Dostupnost – informacije moraju ispitaniku biti lako dostupne.
- Kontekstualnost – informacije bi se trebale dostaviti u odgovarajućem trenutku i u odgovarajućem obliku.
- Relevantnost – informacije bi trebale biti relevantne i primjenjive na određenog ispitanika.
- Univerzalni dizajn – informacije moraju biti dostupne svim ispitanicima, uključivati uporabu strojno čitljivih jezika kako bi se olakšale i automatizirale čitljivost i jasnoća.
- Razumljivo – ispitanici bi trebali dobro razumjeti ono što mogu očekivati u vezi s obradom svojih osobnih podataka, posebno kada su ispitanici djeca ili druge ranjive skupine.
- Dostupnost putem više kanala – informacije bi se trebale dostavljati različitim kanalima i u različitim medijima, a ne samo u tekstnom obliku, kako bi se povećala vjerojatnost da će informacije uspješno doći do ispitanika.
- Slojevit pristup – struktura informacija trebala bi biti višeslojna kako bi one istodobno bile potpune i razumljive te ispunile razumna očekivanja ispitanika.

Primjer:[25]

Voditelj obrade na svojim internetskim stranicama izrađuje pravila zaštite privatnosti kako bi ispunio zahtjeve u pogledu transparentnosti. Pravila zaštite privatnosti ne bi trebala sadržavati opsežne informacije koje su prosječnom ispitaniku nejasne i teško razumljive. Moraju biti jasno i sažeto napisana kako bi korisnici internetskih stranica lako razumjeli na koji se način obrađuju njihovi osobni podatci. Stoga voditelj obrade iznosi informacije slojevito, pri čemu ističe najvažnije činjenice. Omogućuje se jednostavan pristup detaljnijim informacijama. Postavljeni su padajući izbornici i navedene poveznice na druge stranice kako bi se dodatno objasnile različite stavke i pojmovi koji se upotrebljavaju u pravilima. Osim toga, voditelji obrade osiguravaju da se informacije pružaju na više načina, u obliku videoisječaka kojima se objašnjavaju najvažniji elementi informacija iznesenih u pisanom obliku. Sinergija među različitim stranicama ključna je kako bi se slojevitim pristupom potencijalne nejasnoće smanjile, a ne povećale.

Pravila zaštite privatnosti ispitanicima ne bi trebala biti teško dostupna. Pravila zaštite privatnosti dostupna su i vidljiva na svim stranicama određenog mrežnog mjesta, tako da ispitanika uvijek od pristupa informacijama dijeli samo jedan klik. Dostavljene informacije isto su tako osmišljene u skladu s najboljom praksom i standardima jedinstvenog dizajna kako bi bile dostupne svima.

Nadalje, potrebne informacije trebale bi se dostaviti u pravom kontekstu i u odgovarajuće vrijeme. Budući da voditelj obrade mnoge postupke obrade provodi s pomoću podataka prikupljenih na internetskim stranicama, opća pravila zaštite privatnosti na internetskim stranicama sama po sebi nisu dovoljna da bi voditelj obrade ispunio zahtjeve u pogledu transparentnosti. Voditelji obrade stoga oblikuju protok informacija, s pomoću kojih upoznaju ispitanike s relevantnim informacijama u odgovarajućem kontekstu upotrebljavajući npr. informativne isječke ili skočne prozore. Na primjer, ako

[25] Francusko tijelo za zaštitu podataka objavilo je nekoliko primjera najbolje prakse u informiranju korisnika te druga načela transparentnosti: https://design.cnil.fr/en/

se od ispitanika traži da unese osobne podatke, voditelj obrade obavješćuje ispitanika o tome kako će se ti osobni podatci obrađivati i zašto su osobni podatci potrebni za obradu.

3.2 Zakonitost

67. Voditelj obrade mora utvrditi valjanu pravnu osnovu za obradu osobnih podataka. Mjerama i zaštitnim mjerama trebalo bi poduprijeti zahtjev da se osigura da cijeli životni ciklus obrade bude u skladu s relevantnom pravnom osnovom za obradu.

68. Ključni tehnički i integrirani elementi zakonitosti mogu biti sljedeći:
    - Relevantnost – na obradu se primjenjuje pravilna pravna osnova.
    - Diferencijacija[26] – pravna osnova koja se primjenjuje za svaku aktivnost obrade mora se razlikovati.
    - Određena svrha – odgovarajuća pravna osnova mora biti jasno povezana s posebnom svrhom obrade[27].
    - Nužnost – kako bi bila zakonita, obrada mora biti nužna i bezuvjetna.
    - Autonomija – ispitanicima bi se trebala dodijeliti najviša moguća razina autonomije kad je riječ o nadzoru nad osobnim podatcima u okvirima pravne osnove.
    - Dobivanje privole – privola mora biti dobrovoljna, posebna, informirana i nedvosmislena[28]. Posebno bi se trebala razmotriti sposobnost djece i mladih osoba da daju informiranu privolu.
    - Povlačenje privole – ako je privola pravna osnova, u okviru obrade trebalo bi se olakšati povlačenje privole. Povlačenje privole mora biti jednako lako kao i davanje privole. Ako nije tako, mehanizam za davanje privole voditelja obrade nije u skladu s Općom uredbom o zaštiti podataka[29].
    - Odvagivanje interesa – ako su legitimni interesi pravna osnova, voditelj obrade mora precizno odvagati interese i pritom posebno razmotriti neravnotežu moći, konkretno u slučaju djece mlađe od 18 godina i drugih ranjivih skupina. Moraju biti uspostavljene mjere i zaštitne mjere za ublažavanje negativnog učinka na ispitanike.
    - Prethodno utvrđivanje – pravna osnova utvrđuje se prije početka obrade.
    - Prestanak – ako pravna osnova prestane važiti, u skladu s time obrada se prekida.
    - Prilagodba – ako postoji valjana promjena pravne osnove za obradu, stvarna obrada mora se prilagoditi u skladu s novom pravnom osnovom[30].
    - Raspodjela odgovornosti – ako je predviđen zajednički nadzor, strane moraju jasno i transparentno raspodijeliti svoje odgovornosti prema ispitaniku i u skladu s tom raspodjelom osmisliti mjere obrade.

Primjer:

[26] Europski odbor za zaštitu podataka. „Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima". Verzija 2.0, 8. listopada 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_hr.pdf

[27] Vidjeti odjeljak u nastavku koji se odnosi na ograničavanje svrhe.

[28] Vidjeti Smjernice 05/2020 o privoli na temelju Uredbe 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Vidjeti Smjernice 05/2020 o privoli na temelju Uredbe 2016/679, str. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Ako je izvorna pravna osnova privola, vidjeti Smjernice 05/2020 o privoli na temelju Uredbe 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Banka planira ponuditi uslugu za poboljšanje učinkovitosti upravljanja zahtjevima za zajam. Ta se usluga temelji na zamisli prema kojoj banka, nakon što od klijenta zatraži dopuštenje, može izravno od javnog poreznog tijela dobiti podatke o klijentu. U tom se primjeru ne uzima u obzir obrada osobnih podataka iz drugih izvora.

Nužno je pribaviti osobne podatke o financijskom stanju ispitanika kako bi se na zahtjev ispitanika prije sklapanja ugovora o zajmu mogli poduzeti određeni koraci[31]. Međutim, prikupljanje osobnih podataka izravno od porezne uprave ne smatra se nužnim jer klijent pri sklapanju ugovora može sam dati informacije koje posjeduje porezna uprava. Iako banka može imati legitiman interes za prikupljanje dokumentacije izravno od poreznih tijela, na primjer, kako bi se osigurala učinkovita obrada zahtjeva za odobravanje zajma, takav izravan pristup banke osobnim podatcima podnositelja zahtjeva predstavlja rizik za uporabu ili moguću zloporabu prava pristupa.

Pri provedbi načela zakonitosti voditelj obrade uvidjet će da u tom kontekstu ne može primjenjivati razlog „potrebno za ugovor" za dio obrade koji uključuje prikupljanje osobnih podataka izravno od poreznih tijela. Činjenica da takva određena obrada predstavlja rizik da ispitanici budu manje uključeni u obradu svojih podataka također je važan čimbenik ocjene zakonitosti same obrade. Banka zaključuje da se taj dio obrade mora temeljiti na nekoj drugoj pravnoj osnovi obrade. U konkretnoj državi članici u kojoj se nalazi voditelj obrade na snazi su nacionalni zakoni kojima se banci dopušta da prikuplja informacije izravno od javnih poreznih tijela ako ispitanik za to prethodno dâ privolu.

Banka stoga pruža informacije o obradi na internetskoj platformi za podnošenje zahtjeva na način kojim se ispitanicima olakšava razumijevanje toga koji je dio obrade obvezan, a koji nije. Mogućnosti obrade automatski ne omogućuju učitavanje podataka izravno iz drugih izvora osim od samog ispitanika, a opcija za izravno dohvaćanje informacija prikazana je na način koji ne odvraća ispitanika od suzdržavanja. Svaka privola za prikupljanje podataka izravno od drugih voditelja obrade jest privremeno pravo pristupa određenoj skupini podataka.

Svaka se privola obrađuje elektronički na način tako da omogućuje dokumentiranje, a ispitanici mogu jednostavno kontrolirati ono na što su pristali i povući svoju privolu.

Voditelj obrade prethodno je procijenio zahtjeve tehničke i integrirane zaštite podataka i u zahtjeve natječaja za nabavu platforme uključuje sve navedene kriterije. Voditelj obrade svjestan je da ako u natječaj ne uključi zahtjeve tehničke i integrirane zaštite podataka, to može dovesti do zakašnjelog ili vrlo skupog postupka za naknadnu provedbu zaštite podataka.

3.3 Poštenost

69. Poštenost je sveobuhvatno načelo kojim se zahtijeva da se osobni podatci ne obrađuju na način koji je neopravdano štetan, nezakonito diskriminirajući, neočekivan ili obmanjujući za ispitanika. Mjerama i zaštitnim mjerama za provedbu načela poštenosti također se podupiru prava i slobode ispitanikâ, a posebno pravo na informiranje (transparentnost), pravo na intervenciju (pristup, brisanje, prenosivost podataka, ispravljanje) i pravo na ograničavanje obrade (pravo da se na njega ne primjenjuje automatizirano pojedinačno donošenje odluka i nediskriminacija ispitanikâ u takvim postupcima).

70. Ključni tehnički i integrirani elementi poštenosti mogu biti sljedeći:
    - Autonomija – ispitanicima bi se trebala dodijeliti najviša moguća razina autonomije kad je riječ o odlučivanju o uporabi njihovih osobnih podataka te opsegu i uvjetima te uporabe ili obrade.

[31] Vidjeti članak 6. stavak 1. točku (b) Opće uredbe o zaštiti podataka.

- Interakcija – ispitanici moraju moći komunicirati o svojim pravima u kontekstu obrade osobnih podataka koju provodi voditelj obrade te ostvarivati svoja prava u tom pogledu.
- Očekivanja – obrada bi trebala biti u skladu s očekivanjima ispitanika.
- Nediskriminacija – voditelj obrade ne smije nepošteno diskriminirati ispitanike.
- Neiskorištavanje – voditelj obrade ne bi smio iskorištavati potrebe ili ranjivost ispitanika.
- Odabir potrošača – voditelj obrade ne smije nepošteno „zaključati" svoje korisnike. Ako je riječ o vlasničkoj usluzi obrade osobnih podataka, može nastati učinak zaključavanja u okviru te usluge, što može biti nepošteno ako se time ispitanicima onemogućuje da ostvaruju svoje pravo prenosivosti podataka u skladu s člankom 20.
- Ravnoteža moći – ravnoteža moći trebala bi biti ključan cilj odnosa između voditelja obrade i ispitanika. Trebalo bi izbjegavati svaki oblik neravnoteže moći. Kad to nije moguće, trebalo bi je prepoznati i poduzeti odgovarajuće protumjere.
- Zabrana prijenosa rizika – voditelji obrade ne smiju na ispitanike prenositi rizike povezane s poduzećem.
- Zabrana obmanjivanja – informacije o obradi podataka i mogućnosti za njihovu obradu trebale bi se iznositi na objektivno i neutralno, tako da se izbjegne svaka vrsta obmanjujućeg ili manipulativnog jezika ili dizajna.
- Poštovanje prava – voditelj obrade mora poštovati temeljna prava ispitanika i provoditi odgovarajuće mjere i zaštitne mjere. U ta se prava ne smije zadirati ako to nije izričito opravdano zakonom.
- Etičnost – voditelj obrade trebao bi sagledati širi utjecaj obrade na prava i dostojanstvo pojedinaca.
- Istinitost – voditelj obrade mora staviti na raspolaganje informacije o načinu na koji obrađuje osobne podatke. Trebao bi postupati kako je predvidio i ne smije obmanjivati ispitanike.
- Ljudska intervencija – voditelj obrade mora uključiti *kvalificiranu* ljudsku intervenciju kojom se mogu otkriti potencijalne pristranosti strojeva u skladu s pravom ispitanika na to da ne podliježu automatiziranom pojedinačnom donošenju odluka iz članka 22.[32]
- Pošteni algoritmi – nužno je redovito procjenjivati funkcioniraju li algoritmi u skladu s predviđenim svrhama te prilagođavati algoritme kako bi se ublažio učinak otkrivenih pristranosti i osigurala poštena obrada. Ispitanike bi trebalo obavijestiti o načinu na koji obrada osobnih podataka funkcionira na temelju algoritama s pomoću kojih se analiziraju ispitanici ili na temelju kojih se o njima donose predviđanja, kao što su radna uspješnost, ekonomsko stanje, zdravlje, osobne preferencije, pouzdanost ili ponašanje, lokacija ili kretanja[33].

Primjer 1.

Voditelj obrade upravlja tražilicom koja uglavnom obrađuje osobne podatke koje su izradili korisnici. Voditelj obrade ima koristi od velikih količina osobnih podataka i može te osobne podatke upotrijebiti za ciljane oglase. Voditelj obrade stoga želi utjecati na ispitanike kako bi se omogućilo opsežnije prikupljanje i uporaba njihovih osobnih podataka. Privola bi se trebala pribaviti tako da se ispitaniku iznesu mogućnosti obrade.

[32] Vidjeti Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679 https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Vidjeti uvodnu izjavu 71. Opće uredbe o zaštiti podataka.

Pri provedbi načela poštenosti, uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade, voditelj obrade shvaća da ne može predstaviti mogućnosti na način kojim bi se ispitanici potaknuli na djelovanje u smjeru koji bi voditelju obrade omogućio da prikuplja više osobnih podataka nego onda kada bi se mogućnosti predstavile na jednak i neutralan način. To znači da ne mogu predstaviti mogućnosti obrade tako da se ispitanicima oteža suzdržavanje od dijeljenja vlastitih podataka ili prilagodba vlastitih postavki privatnosti te time i ograničavanje obrade. To su primjeri prijevara putem sučelja (tzv. *dark patterns*) koji su u suprotnosti s člankom 25. Zadane mogućnosti obrade ne bi trebale biti invazivne, a mogućnosti odabira za daljnju obradu trebale bi biti predočene tako da se na ispitanika ne vrši pritisak za davanje privole. Stoga voditelj obrade prikazuje mogućnosti za davanje privole ili suzdržavanje od sudjelovanja kao dvije jednako vidljive mogućnosti u okviru kojih se ispitaniku precizno navode posljedice svakog od tih odabira.

Primjer 2.

Drugi voditelj obrade obrađuje osobne podatke za pružanje usluge internetskog prijenosa pri čemu korisnici mogu birati između redovite pretplate standardne kvalitete i posebne pretplate bolje kvalitete. Kao dio posebne pretplate, pretplatnici dobivaju prednost kod određenih usluga za korisnike.

Kad je riječ o načelu poštenosti, prednost koju dobivaju korisnici s posebnom pretplatom ne smije dovesti do diskriminacije korisnika s redovitom pretplatom pri ostvarivanju njihovih prava u skladu s člankom 12. Opće uredbe o zaštiti podataka. To znači da, iako korisnici posebne pretplate imaju prednost kod određenih usluga, takvo davanje prednosti ne smije dovesti do nedostatka odgovarajućih mjera za odgovor na zahtjev redovnih pretplatnika bez nepotrebnog odgađanja, a u svakom slučaju u roku od mjesec dana od primitka zahtjeva.

Korisnici s posebnom pretplatom mogu platiti za bolju uslugu, ali svi ispitanici moraju imati jednak i neselektivan pristup ostvarivanju svojih prava i sloboda u skladu s člankom 12.

3.4 Ograničavanje svrhe[34]

71. Voditelj obrade mora prikupljati podatke za posebne, izričite i zakonite svrhe, a ne dalje obrađivati podatke na način koji nije u skladu sa svrhama za koje su prikupljeni[35]. Strukturu obrade stoga treba oblikovati na temelju onoga što je nužno za postizanje svrhe. Ako dođe do daljnje obrade, voditelj obrade najprije mora provjeriti jesu li svrhe obrade u skladu s izvornima te u skladu s time osmisliti takvu obradu. U skladu s kriterijima iz članka 6. stavka 4. ocjenjuje se je li nova svrha usklađena ili ne.

72. Ključni tehnički i integrirani elementi ograničavanja svrhe mogu biti sljedeći:
- Prethodno utvrđivanje – zakonite svrhe moraju se utvrditi prije osmišljavanja obrade.
- Posebnost – svrhe obrade osobnih podataka moraju biti posebno i izričito navedene.
- Usmjerenost na svrhu – svrha obrade trebala bi usmjeravati strukturu obrade i na njoj bi se trebale temeljiti granice obrade.

[34] Radna skupina iz članka 29. iznijela je upute za razumijevanje načela ograničavanja svrhe iz Direktive 95/46/EZ. Iako Europski odbor za zaštitu podataka nije usvojio ovo mišljenje, ono unatoč tomu može biti relevantno jer je tekst načela isti kao u Općoj uredbi o zaštiti podataka. Radna skupina iz članka 29. „Mišljenje 03/2013 o ograničavanju svrhe". WP 203, 2. travnja 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Članak 5. stavak 1. točka (b) Opće uredbe o zaštiti podataka.

- Nužnost– na temelju svrhe određuje se koji su osobni podatci potrebni za obradu.
- Kompatibilnost – svaka nova svrha mora biti u skladu s izvornom svrhom za koju su podatci prikupljeni te se na njoj moraju temeljiti relevantne promjene u strukturi.
- Ograničenje daljnje obrade – voditelj obrade ne bi trebao povezivati skupove podataka ili obavljati daljnju obradu za nove neusklađene svrhe.
- Ograničenja ponovne uporabe – voditelj obrade trebao bi upotrebljavati tehničke mjere, uključujući raspršeno adresiranje (eng. *hashing*) i šifriranje kako bi ograničio mogućnost prenamjene osobnih podataka. Voditelj obrade trebao bi imati uspostavljene i organizacijske mjere, kao što su politike i ugovorne obveze, kojima se ograničava ponovna uporaba osobnih podataka.
- Preispitivanje – voditelj obrade trebao bi redovito preispitivati je li neka obrada potrebna u svrhe za koje su podatci prikupljeni i ispitivati strukturu u odnosu na ograničavanje svrhe.

Primjer:

Voditelj obrade obrađuje osobne podatke o svojim klijentima. Svrha je obrade izvršavanje ugovora, tj. mogućnost isporuke robe na točnu adresu i provedba plaćanja. Pohranjeni osobni podatci odnose se na povijest kupnje, ime, adresu, e-poštu te broj telefona.

Voditelj obrade razmišlja o kupnji proizvoda za upravljanje odnosima s klijentima u sklopu kojeg se svi podatci o klijentima koji se odnose na prodaju, marketing i službu za korisnike prikupljaju na jednom mjestu. Proizvod omogućuje pohranu svih telefonskih poziva, aktivnosti, dokumenata, e-pošte i marketinških kampanja kako bi se dobio cjelovit pregled klijenta. Nadalje, u sklopu tog proizvoda za upravljanje odnosima s klijentima s pomoću javnih informacija može se automatski analizirati kupovna moć klijenata. Svrha je analize bolje usmjeravanje aktivnosti oglašavanja. Te aktivnosti nisu obuhvaćene izvornom zakonitom svrhom obrade.

Kako bi poštovao načelo ograničavanja svrhe, voditelj obrade od pružatelja proizvoda zahtijeva povezivanja različitih aktivnosti obrade u kojima se osobni podatci upotrebljavaju s potrebama koje su voditelju obrade bitne.

Nakon što dobije rezultate tog povezivanja, voditelj obrade procjenjuje jesu li nova marketinška svrha i svrha ciljanog oglašavanja u skladu s izvornim svrhama koje su utvrđene u trenutku prikupljanja podataka te postoji li dostatna pravna osnova za predmetnu obradu. Ako rezultat procjene ne bude pozitivan, voditelj obrade ne smije nastaviti upotrebljavati te funkcije. Umjesto toga, voditelj obrade mogao bi odustati od procjene i jednostavno ne upotrebljavati opisane funkcije proizvoda.

3.5 Smanjenje količine podataka

73. Obrađuju se samo osobni podatci koji su primjereni, relevantni i ograničeni na ono što je **nužno** za tu svrhu[36]. Zbog toga voditelj obrade mora unaprijed odrediti koja su obilježja i parametri sustavâ za obradu te njihove pomoćne funkcije dopušteni. Smanjenjem količine podataka potvrđuje se i provodi načelo nužnosti. U daljnjoj obradi voditelj obrade trebao bi redovito razmatrati jesu li obrađeni osobni podatci i dalje primjereni, relevantni i nužni ili se podatci brišu ili anonimiziraju.

74. Voditelji obrade trebali bi prije svega utvrditi trebaju li uopće obrađivati osobne podatke u njihove relevantne svrhe. Voditelj obrade trebao bi provjeriti mogu li se ostvariti relevantne svrhe tako da se

[36] Članak 5. stavak 1. točka (c) Opće uredbe o zaštiti podataka.

obrađuje manja količina osobnih podataka ili tako da se prikupe manje detaljni ili agregirani osobni podatci ili pak tako da se uopće ne obrađuju osobni podatci[37]. Takva bi se provjera trebala provesti prije nego što započne postupak obrade, no mogla bi se provesti i u bilo kojem trenutku tijekom životnog ciklusa obrade. To je također u skladu s člankom 11.

75. Smanjenje se može odnositi i na stupanj identifikacije. Ako svrha obrade ne zahtijeva da se konačnim skupom podataka uputi na pojedinca čiji je identitet utvrđen ili se može utvrditi (npr. u statistici), ali prvobitnom se obradom podataka to čini (npr. prije agregiranja podataka), voditelj obrade briše ili anonimizira osobne podatke čim identifikacija više nije potrebna. Ako je nastavak identifikacije potreban za druge aktivnosti obrade, osobni podatci trebali bi se pseudonimizirati kako bi se ublažili rizici za prava ispitanika.

76. Ključni tehnički i integrirani elementi smanjenja količine podataka mogu biti sljedeći:
    - Izbjegavanje podataka – izbjegavajte obradu osobnih podataka kada god je to moguće u relevantnu svrhu.
    - Ograničavanje – ograničite količinu prikupljenih osobnih podataka na onu koja je nužna za tu svrhu.
    - Ograničenje pristupa – organizirajte obradu podataka tako da minimalan broj osoba treba pristup osobnim podatcima za izvršavanje svojih dužnosti te u skladu s time ograničite pristup.
    - Relevantnost – osobni podatci trebali bi biti relevantni za predmetnu obradu, a voditelj obrade trebao bi moći dokazati tu relevantnost.
    - Nužnost – svaka kategorija osobnih podataka potrebna je u određene svrhe i treba se obrađivati samo ako tu svrhu nije moguće ostvariti drugim sredstvima.
    - Agregiranje – kada je to moguće, upotrijebite agregirane podatke.
    - Pseudonimizacija – pseudonimizirajte osobne podatke čim više nije potrebno imati osobne podatke kojima se omogućuje izravno utvrđivanje identiteta pojedinaca i odvojeno pohranjujte identifikacijske ključeve.
    - Anonimizacija i brisanje – ako osobni podatci nisu potrebni ili nisu više potrebni u tu svrhu, osobni podatci anonimiziraju se ili brišu.
    - Protok podataka – protok podataka trebao bi biti dovoljno učinkovit da se pritom ne izradi više kopija nego što je nužno.
    - Najnovija dostignuća – voditelj obrade trebao bi primijeniti suvremene i prikladne tehnologije za izbjegavanje podataka i smanjenje količine podataka.

Primjer 1.

Knjižara želi povećati svoje prihode prodajom knjiga na internetu. Vlasnik knjižare želi uspostaviti standardizirani obrazac za postupak naručivanja. Kako bi se osiguralo da kupci unesu sve željene informacije, vlasnik knjižare sva polja na obrascu označava kao obvezna (ako ne ispuni sva polja, kupac ne može poslati narudžbu). Vlasnik internetske trgovine u početku upotrebljava standardni obrazac za kontakt u kojem se od kupca traži da unese podatke kao što su datum rođenja, telefonski broj i kućna adresa. Međutim, nisu sva polja u obrascu nužna za kupnju i isporuku knjiga. U tom konkretnom slučaju, ako ispitanik proizvod plaća unaprijed, datum rođenja i telefonski broj ispitanika nisu nužni podatci za kupnju proizvoda. To znači da ta polja na internetskom obrascu ne mogu biti obvezna pri

[37] U uvodnoj izjavi 39. Opće uredbe o zaštiti podataka navodi se sljedeće: „Osobni podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima."

naručivanju proizvoda, osim ako voditelj obrade može jasno dokazati da su ti podatci nužni za druge svrhe zbog kojih su ta polja obvezna. Osim toga, postoje situacije u kojima ni adresa nije potrebna. Na primjer, pri naručivanju e-knjige kupac može preuzeti proizvod izravno na svoj uređaj.

Vlasnik internetske trgovine stoga odlučuje izraditi dva obrasca: jedan za naručivanje knjiga, s poljem za adresu kupca, i jedan internetski obrazac za naručivanje e-knjiga, bez polja za adresu kupca.

Primjer 2.

Poduzeće javnog prijevoza želi prikupljati statističke podatke na temelju ruta putnika. To je korisno za potrebe pravilnog odabira promjena voznog reda javnog prijevoza i odgovarajuće rute vlakova. Putnici moraju provući svoje karte kroz čitač pri svakom ulasku ili izlasku iz prijevoznog sredstva. Nakon što je proveo procjenu rizika povezanih s pravima i slobodama putnika u pogledu prikupljanja podataka o rutama putovanja putnika, voditelj obrade utvrđuje da je identitet putnika, u slučajevima u kojima oni žive ili rade u slabije naseljenim područjima, moguće utvrditi na temelju samo jedne identifikacije rute s pomoću identifikatora karata. Stoga, s obzirom na to da nije potreban za optimizaciju voznog reda javnog prijevoza i ruta vlakova, voditelj obrade ne pohranjuje podatke prikupljene s pomoću identifikatora karata. Nakon završetka putovanja voditelj obrade pohranjuje samo pojedinačne rute putovanja kako ne bi mogao identificirati putovanja povezana s jednom kartom, a zadržava samo informacije o odvojenim rutama putovanja.

U slučajevima u kojima i dalje može postojati rizik od utvrđivanja identiteta osobe samo na temelju njezine rute putovanja javnim prijevozom, voditelj obrade provodi statističke mjere za smanjenje rizika, kao što su izostavljanje početka i završetka rute.

Primjer 3.

Dostavljač želi procijeniti učinkovitost svojih isporuka u pogledu vremena dostave, rasporeda radnog opterećenja i potrošnje goriva. Kako bi se taj cilj postigao, dostavljač mora obraditi niz osobnih podataka koji se odnose i na zaposlenike (vozače) i kupce (adrese, proizvodi koji se dostavljaju itd.). Postupak obrade podrazumijeva rizike od praćenja zaposlenika, za što su potrebne posebne pravne zaštitne mjere, i praćenja navika kupaca kroz saznanja o isporučenim proizvodima tijekom vremena. Ti se rizici mogu znatno smanjiti uz odgovarajuću pseudonimizaciju zaposlenika i kupaca. Posebno ako se ključevi za pseudonimizaciju često mijenjaju i u obzir se uzimaju samo makropodručja umjesto detaljnih adresa, uspijeva se postići učinkovito smanjenje količine podataka, a voditelj obrade može se usredotočiti samo na postupak isporuke i na svrhu optimizacije resursa, bez prelaska praga za praćenje ponašanja pojedinaca (kupaca ili zaposlenika).

Primjer 4.

Bolnica prikuplja podatke o svojim pacijentima u okviru bolničkog informacijskog sustava (elektronička zdravstvena evidencija). Osoblje bolnice treba pristupiti kartonima pacijenata kako bi moglo donijeti informirane odluke o skrbi za pacijente i njihovu liječenju te kako bi evidentiralo sve mjere poduzete u pogledu dijagnoze, skrbi i liječenja. U skladu s integriranim pravilima pristup se odobrava automatski samo članovima medicinskog osoblja koji su zaduženi za liječenje određenog pacijenta u

specijaliziranom odjelu na koji je taj pacijent raspoređen. Skupina osoba s pristupom kartonu pacijenta povećava se ako se u liječenje uključe drugi odjeli ili dijagnostičke jedinice. Nakon otpuštanja pacijenta s odjela i dovršetka postupka izdavanja računa, pristup se ograničava na malenu skupinu zaposlenika po specijaliziranom odjelu koji odgovaraju na zahtjeve za medicinske informacije ili savjetovanje koje provode ili traže drugi pružatelji medicinskih usluga na temelju odobrenja predmetnog pacijenta.

3.6 Točnost

77. Osobni podatci moraju biti točni i ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podatci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave[38].

78. Zahtjeve bi se trebalo promatrati u odnosu na rizike i posljedice konkretne uporabe podataka. Netočni osobni podatci mogli bi predstavljati rizik za prava i slobode ispitanikâ, na primjer kada dovode do neispravne dijagnoze ili pogrešne obrade nekog zdravstvenog protokola ili kada netočna predodžba o nekoj osobi može dovesti do toga da se odluke donose na pogrešnoj osnovi ili na temelju automatiziranog donošenja odluka ili s pomoću umjetne inteligencije.

79. Ključni tehnički i integrirani elementi točnosti mogu biti sljedeći:
    - Izvor podataka – izvori osobnih podataka trebali bi biti pouzdani u smislu točnosti podataka.
    - Stupanj točnosti – svaki element osobnih podataka trebao bi biti onoliko točan koliko je potrebno za određene svrhe.
    - Mjerljiva točnost – mora se smanjiti količina lažno pozitivnih/negativnih rezultata, na primjer, zbog pristranosti u sklopu automatiziranog donošenja odluka i umjetne inteligencije.
    - Provjera – ovisno o prirodi podataka i o tome koliko se često ti podatci mogu promijeniti, voditelj obrade trebao bi prije obrade i u različitim fazama obrade s ispitanikom provjeriti točnost osobnih podataka (npr. zahtjevi u pogledu starosne dobi).
    - Brisanje/ispravak – voditelj obrade mora bez odlaganja izbrisati ili ispraviti netočne podatke. Voditelj obrade mora taj postupak posebno olakšati ako su ispitanici djeca i ako oni naknadno žele ukloniti takve osobne podatke[39].
    - Izbjegavanje propagacije pogrešaka – voditelji obrade trebali bi ublažiti učinak akumulirane pogreške u lancu obrade.
    - Pristup – ispitanicima bi trebalo dostaviti informacije o osobnim podatcima i omogućiti učinkovit pristup takvim podatcima u skladu s člancima 12. i 15. Opće uredbe o zaštiti podataka kako bi mogli nadzirati njihovu točnost i ispraviti ih prema potrebi.
    - Kontinuirana točnost – osobni podatci trebali bi biti točni u svim fazama obrade, a ispitivanja točnosti trebala bi se provoditi tijekom kritičnih koraka.
    - Ažurnost – osobni se podatci ažuriraju ako je to potrebno za određenu svrhu.
    - Dizajn podataka – upotrijebite tehnološke i organizacijske značajke dizajna kako biste smanjili netočnost, na primjer, umjesto polja za slobodan unos teksta ponudite kratke unaprijed definirane mogućnosti za odabir.

Primjer 1.

Osiguravajuće društvo želi upotrijebiti umjetnu inteligenciju za izradu profila klijenata koji kupuju osiguranje, koji će im služiti kao osnova za donošenje odluka pri izračunu rizika osiguranja. Pri utvrđivanju načina na koji bi se trebala razvijati njihova rješenja umjetne inteligencije, određuju se

[38] Članak 5. stavak 1. točka (d) Opće uredbe o zaštiti podataka.
[39] Usp. uvodnu izjavu 65.

načini obrade, a pri odabiru aplikacije umjetne inteligencije od prodavatelja mora se uzeti u obzir tehnička zaštita podataka, kao i pri odabiru načina treniranja algoritama umjetne inteligencije.

Pri utvrđivanju načina treniranja algoritama umjetne inteligencije, voditelj obrade trebao bi imati točne podatke za postizanje preciznih rezultata. Stoga bi voditelj obrade trebao osigurati točnost podataka koji se upotrebljavaju za treniranje algoritama umjetne inteligencije.

Ako postoji valjana pravna osnova za treniranje algoritama umjetne inteligencije s pomoću osobnih podataka iz velike podskupine postojećih klijenata, voditelj obrade odabire skupinu klijenata koja je reprezentativna za određenu populaciju kako bi isto tako izbjegao pristranost.

Podatci klijenata zatim se prikupljaju iz odgovarajućeg sustava za obradu podataka, uključujući podatke o vrsti osiguranja, npr. zdravstveno osiguranje, osiguranje doma, putno osiguranje itd., te podatke iz javnih registara kojima voditelj obrade može zakonito pristupiti. Prije prijenosa u sustav za treniranje modela umjetne inteligencije svi se podatci pseudonimiziraju.

Kako bi se osiguralo da podatci koji se upotrebljavaju za treniranje algoritama umjetne inteligencije budu što točniji, voditelj obrade prikuplja samo podatke iz izvora podataka s ispravnim i ažuriranim informacijama.

Osiguravajuće društvo ispituje pouzdanost umjetne inteligencije i objavljuje nediskriminirajuće rezultate tijekom izrade proizvoda i konačno prije stavljanja proizvoda na tržište. Nakon što se umjetna inteligencija u potpunosti poduči i pusti u rad, osiguravajuće društvo upotrebljava te rezultate za pomoć pri procjenama rizika povezanih s osiguranjem. No pritom se, kad je riječ o odobrenju osiguranja, ne oslanja isključivo na odluku donesenu s pomoću aplikacije umjetne inteligencije, osim ako je ta odluka donesena u skladu s izuzećima iz članka 22. stavka 2. Opće uredbe o zaštiti podataka.

Isto tako, osiguravajuće društvo redovito će preispitivati rezultate dobivene umjetnom inteligencijom kako bi održavalo odgovarajuću razinu pouzdanosti i prema potrebi prilagođavalo algoritam.

Primjer 2.

Voditelj obrade zdravstvena je ustanova koja želi pronaći metode za osiguravanje cjelovitosti i točnosti osobnih podataka u svojim registrima klijenata.

U situacijama u kojima dvije osobe stižu u ustanovu istodobno i primaju isto liječenje, postoji opasnost da ih se zamijeni ako je ime jedini parametar koji ih razlikuje. Kako bi se osigurala točnost, voditelj obrade treba jedinstveni identifikator za svaku osobu te stoga i više informacija od samog imena klijenta.

Ustanova upotrebljava nekoliko sustava koji sadržavaju osobne podatke klijenata i mora osigurati da su informacije koje se odnose na klijenta točne, precizne i dosljedne u svim sustavima u bilo kojem trenutku. Ustanova je utvrdila nekoliko rizika koji se mogu pojaviti ako se informacije promijene u jednom sustavu, ali ne i u ostalima.

Voditelj obrade odlučuje ublažiti rizik uporabom tehnike raspršivanja koja se može upotrijebiti za osiguravanje cjelovitosti podataka u dnevniku liječenja. Izrađuju se kriptografske vremenske oznake za zapise u dnevniku liječenja i klijenta koji je povezan s tim zapisima kako bi se svaka promjena mogla prepoznati, staviti u korelaciju i prema potrebi pratiti.

3.7 Ograničenje pohrane

80. Voditelj obrade mora osigurati da se osobni podatci čuvaju u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podatci obrađuju[40]. Od ključne je važnosti da voditelj obrade točno zna koje osobne podatke poduzeće obrađuje i zašto. Svrha obrade mora biti glavni kriterij za odlučivanje o tome koliko se dugo ti osobni podatci pohranjuju.

81. Mjere i zaštitne mjere kojima se provodi načelo ograničenja pohrane nadopunjuju prava i slobode ispitanika, a posebno pravo na brisanje i pravo na prigovor.

82. Ključni tehnički i integrirani elementi ograničenja pohrane mogu biti sljedeći:
- Brisanje i anonimizacija – voditelj obrade trebao bi imati uspostavljene jasne interne postupke i funkcije za brisanje i/ili anonimizaciju.
- Učinkovitost anonimizacije/brisanja – voditelj obrade mora se pobrinuti da nije moguće ponovno prepoznati anonimizirane podatke ili obnoviti izbrisane podatke te bi trebao ispitati je li to moguće
- Automatizacija – brisanje određenih osobnih podataka trebalo bi biti automatizirano.
- Kriteriji pohrane – voditelj obrade mora odrediti koji su podatci i trajanje pohrane potrebni za određenu svrhu.
- Obrazloženje – voditelj obrade trebao bi moći obrazložiti zašto je određeno razdoblje pohrane nužno za predmetnu svrhu i predmetne osobne podatke te moći iznijeti razlog i pravnu osnovu za razdoblje zadržavanja.
- Provedba politika zadržavanja – voditelj obrade trebao bi provoditi interne politike zadržavanja i ispitati provodi li organizacija svoje politike.
- Sigurnosne kopije/zapisi – voditelji obrade moraju odrediti koji su podatci i trajanje pohrane nužni za sigurnosne kopije i zapise.
- Protok podataka – voditelji obrade trebali bi voditi računa o protoku osobnih podataka i pohrani svih kopija tih podataka te nastojati ograničiti njihovu „privremenu" pohranu.

Primjer:

Voditelj obrade prikuplja osobne podatke ako je svrha obrade upravljanje članstvom ispitanika. Osobni podatci brišu se nakon prestanka članstva i ne postoji pravna osnova za daljnju pohranu tih podataka.

Voditelj obrade najprije izrađuje interni postupak za zadržavanje i brisanje podataka. U skladu s tim, zaposlenici moraju ručno brisati osobne podatke nakon isteka razdoblja zadržavanja. Zaposlenik prati postupak za redovito brisanje i ispravljanje podataka na svim uređajima, sigurnosnih kopija, zapisa, e-pošte i podataka na drugim odgovarajućim medijima za pohranu.

Kako bi brisanje bilo učinkovitije i manje podložno pogreškama, voditelj obrade zatim umjesto toga uvodi automatski sustav radi automatskog, pouzdanog i redovitijeg brisanja podataka. Sustav je osmišljen tako da slijedi zadani postupak brisanja podataka koji se zatim provodi u unaprijed određenom vremenskom intervalu radi uklanjanja osobnih podataka sa svih medija za pohranu. Voditelj obrade redovito preispituje i ispituje postupak zadržavanja te osigurava da je taj postupak u skladu s ažuriranom politikom zadržavanja.

[40] Članak 5. stavak 1. točka (c) Opće uredbe o zaštiti podataka.

3.8 Cjelovitost i povjerljivost

83. Načelo cjelovitosti i povjerljivosti odnosi se na zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera. Sigurnost osobnih podataka zahtijeva provedbu odgovarajućih mjera osmišljenih kako bi se spriječili incidenti u vezi s povredom podataka i kako bi se upravljalo tim incidentima, kako bi se zajamčili pravilno obavljanje zadaća povezanih s obradom podataka i usklađenost s ostalim načelima te kako bi se olakšalo učinkovito ostvarivanje prava pojedinaca.

84. U uvodnoj izjavi 78. navodi se da bi se jedna od mjera tehničke i integrirane zaštite podataka mogla sastojati od toga da se voditelju obrade omogući da „stvara i poboljšava sigurnosne značajke". Uz ostale mjere tehničke i integrirane zaštite podataka, u uvodnoj izjavi 78. upućuje se na odgovornost voditelja obrade da kontinuirano procjenjuju upotrebljavaju li se u svakom trenutku odgovarajući načini obrade te da procjenjuju odgovara li se odabranim mjerama na postojeće slabosti. Nadalje, voditelji obrade trebali bi redovito preispitivati mjere sigurnosti informacija u kontekstu osobnih podataka i njihove zaštite te postupak za rješavanje povreda podataka.

85. Ključni tehnički i integrirani elementi cjelovitosti i povjerljivosti mogu biti sljedeći:
    - Sustav upravljanja informacijskom sigurnošću – uspostavljena su operativna sredstva za upravljanje politikama i postupcima za informacijsku sigurnost.
    - Analiza rizika – procijenite rizike za sigurnost osobnih podataka tako da razmotrite učinak na prava pojedinaca i poduzmete mjere za suzbijanje utvrđenih rizika. Kad je riječ o primjeni u procjeni rizika, izradite i održavajte sveobuhvatan, sustavan i realan „model za utvrđivanje prijetnji" i analizu površine napada u okviru za to izrađenog softvera kako biste smanjili vektore napada i mogućnosti za iskorištavanje slabosti i ranjivosti.
    - Tehnička sigurnost – što prije razmotrite sigurnosne zahtjeve u pogledu dizajna i razvoja sustava te kontinuirano integrirajte i provodite odgovarajuća ispitivanja.
    - Održavanje – redovito preispitujte i ispitujte softver, hardver, sustave i usluge itd. kako biste otkrili slabosti sustava koji služe kao pomoć pri obradi.
    - Upravljanje kontrolom pristupa – pristup osobnim podatcima trebalo bi imati samo ovlašteno osoblje koje tim podatcima treba pristupiti radi obavljanja zadaća povezanih s obradom, a voditelj obrade trebao bi razlikovati različite vrste povlaštenog pristupa za ovlašteno osoblje.
        - Ograničenje pristupa (predstavnici) – organizirajte obradu podataka tako da minimalan broj osoba treba pristupiti osobnim podatcima za izvršavanje svojih dužnosti te u skladu s time ograničite pristup.
        - Ograničenje pristupa (sadržaj) – u kontekstu svakog postupka obrade ograničite pristup samo na one atribute po skupu podataka koji su nužni za obavljanje tog postupka. Nadalje, ograničite pristup podatcima na podatke koji se odnose na ispitanike za koje je odgovoran odgovarajući zaposlenik.
        - Odvajanje pristupa – organizirajte obradu podataka tako da nijedna osoba ne treba sveobuhvatan pristup svim podatcima koji su prikupljeni o određenom ispitaniku, a pogotovo svim osobnim podatcima određene kategorije ispitanika.
    - Sigurni prijenosi – prijenosi se moraju zaštititi od neovlaštenog i slučajnog pristupa i promjena.
    - Sigurna pohrana – pohrana podataka mora biti sigurna od neovlaštenog pristupa i promjena. Trebali bi biti uspostavljeni postupci za procjenu rizika povezanih s centraliziranim i decentraliziranim sustavom pohrane te kategorija osobnih podataka na koje se to primjenjuje. Na neke će podatke možda trebati primijeniti dodatne sigurnosne mjere ili će se ti podatci trebati odvojiti od ostalih.

- Pseudonimizacija – osobni podatci i sigurnosne kopije/zapisi trebali bi se pseudonimizirati kao sigurnosna mjera za svođenje rizika od mogućih povreda podataka na najmanju moguću mjeru, na primjer upotrebom raspršivanja ili šifriranja.
- Sigurnosne kopije/zapisi – zadržavanje sigurnosnih kopija i zapisa ako su potrebni za informacijsku sigurnost; upotreba revizijskih tragova i praćenje događaja kao rutinska sigurnosna kontrola. One se moraju zaštititi od neovlaštenog i slučajnog pristupa i promjena te redovito preispitivati, a svi bi se incidenti trebali odmah rješavati.
- Oporavak u slučaju katastrofe / kontinuitet poslovanja – odgovorite na zahtjeve informacijskog sustava u pogledu oporavka u slučaju katastrofe / kontinuiteta poslovanja kako biste ponovno uspostavili dostupnost osobnih podataka nakon velikih incidenata.
- Zaštita u skladu s rizikom – sve kategorije osobnih podataka trebale bi se zaštititi prikladnim mjerama s obzirom na rizik povrede sigurnosti. Podatci koji su podložni posebnim rizicima trebali bi se, kad je to moguće, čuvati odvojeno od ostalih osobnih podataka.
- Upravljanje odgovorima na sigurnosne incidente – uspostavite rutine, postupke i resurse za otkrivanje i suzbijanje povreda podataka, njihovo rješavanje, izvješćivanje o njima i učenje na temelju njih.
- Upravljanje incidentima – voditelj obrade trebao bi uspostaviti postupke za rješavanje povreda i incidenata, kako bi sustav za obradu bio otporniji. To uključuje postupke obavješćivanja kao što je upravljanje obavijestima (za nadzorno tijelo) i informacijama (za ispitanike).

Primjer:

Voditelj obrade želi izdvojiti velike količine osobnih podataka iz medicinske baze podataka u kojoj se nalazi elektronička zdravstvena evidencija (liječnički kartoni pacijenata) na poseban poslužitelj u okviru poduzeća kako bi izdvojene podatke obradio za potrebe osiguranja kvalitete. Poduzeće je procijenilo da je rizik usmjeravanja izdvojenih podataka na poslužitelj koji je dostupan svim zaposlenicima društva vjerojatno visok kad je riječ o pravima i slobodama ispitanika. Budući da u poduzeću postoji samo jedan odjel koji treba obraditi izdvojene podatke pacijenata, voditelj obrade odlučuje pristup posebnom poslužitelju ograničiti na zaposlenike tog odjela. Nadalje, kako bi se dodatno umanjio rizik, podatci će se prije prijenosa pseudonimizirati.

Kako bi se regulirao pristup i ublažila moguća šteta od zlonamjernog softvera, poduzeće odlučuje odvojiti tu mrežu i uspostaviti kontrolu pristupa poslužitelju. Osim toga, uvodi sustav za sigurnosni nadzor te otkrivanje i sprječavanje upada koji odvaja od rutinske uporabe. Uspostavljen je sustav automatizirane revizije radi praćenja pristupa i promjena. Iz tog sustava generiraju se izvješća i automatizirana upozorenja kada se konfiguriraju određeni događaji koji se odnose na uporabu. Voditelj obrade osigurat će da korisnici imaju pristup isključivo na temelju načela nužnog poznavanja i da im se dodijeli odgovarajuća razina pristupa. Neodgovarajuća uporaba može se brzo i jednostavno otkriti.

Neki se izdvojeni podatci moraju usporediti s novima te se stoga moraju pohraniti na tri mjeseca. Voditelj obrade odlučuje te podatke unijeti u zasebne baze podataka na istom poslužitelju i za njihovu pohranu upotrijebiti transparentno šifriranje na razini stupca. Ključevi za dešifriranje podataka u stupcu pohranjuju se u posebnim sigurnosnim modulima koje može upotrebljavati samo ovlašteno osoblje, ali se ne mogu izdvajati.

Rješavanjem incidenata koji se pojavljuju sustav postaje otporniji i pouzdaniji. Voditelj obrade shvaća da bi preventivne i učinkovite mjere te zaštitne mjere trebale biti uključene u sve postupke obrade osobnih podataka sada i u budućnosti te da bi to moglo pomoći u sprječavanju budućih incidenata koji se odnose na povredu osobnih podataka.

Voditelj obrade utvrđuje takve sigurnosne mjere kako bi se osigurala točnost, cjelovitost i povjerljivost, ali i kako bi se spriječilo širenje zlonamjernog softvera kibernapadima, kao i da bi se rješenje učinilo otpornim. Pouzdane sigurnosne mjere pomoći će vam da izgradite povjerenje s ispitanicima.

3.9 Odgovornost[41]

86. U skladu s načelom odgovornosti voditelj obrade odgovoran je za usklađenost sa svim spomenutim načelima i mora dokazati tu usklađenost.

87. Voditelj obrade treba moći dokazati usklađenost s tim načelima. Pritom može dokazati da su mjere koje je poduzeo kako bi zaštitio prava ispitanika proizvele određene učinke i pokazati zašto se te mjere smatraju odgovarajućima i učinkovitima. Na primjer, može pokazati zašto je određena mjera odgovarajuća za učinkovito osiguravanje provedbe načela ograničenja pohrane.

88. Kako bi mogao odgovorno obrađivati osobne podatke, voditelj obrade trebao bi biti upoznat sa zaštitom podataka i biti sposoban za njezinu provedbu. To podrazumijeva da bi voditelj obrade trebao razumjeti obveze u pogledu zaštite podataka iz Opće uredbe o zaštiti podataka i moći ispuniti te obveze.

4 CERTIFICIRANJE NA TEMELJU ČLANKA 25. STAVKA 3.

89. U skladu s člankom 25. stavkom 3. certificiranje na temelju članka 42. može se upotrijebiti kao element za dokazivanje usklađenosti s tehničkom i integriranom zaštitom podataka. S druge strane, dokumenti kojima se dokazuje usklađenost s tehničkom i integriranom zaštitom podataka isto tako mogu biti korisni u postupku certificiranja. To znači da, ako je postupak obrade koji je proveo voditelj obrade ili izvršitelj obrade certificiran u skladu s člankom 42., nadzorna tijela uzimaju to u obzir pri procjeni usklađenosti s Općom uredbom o zaštiti podataka, posebno u pogledu tehničke i integrirane zaštite podataka.

90. Ako je postupak obrade koji provodi voditelj obrade ili izvršitelj obrade certificiran u skladu s člankom 42., elementi koji pomažu dokazati usklađenost s člankom 25. stavcima 1. i 2. jesu tehnički postupci, odnosno postupci za utvrđivanje načina obrade i upravljanja te tehničkih i organizacijskih mjera za provedbu načela zaštite podataka. Kriterije certificiranja zaštite podataka utvrđuju certifikacijska tijela ili vlasnici programa certificiranja, a zatim ih odobrava nadležno nadzorno tijelo ili Europski odbor za zaštitu podataka. Za dodatne informacije o mehanizmima certificiranja vidjeti Smjernice Europskog odbora za zaštitu podataka o certificiranju[42] i druge relevantne smjernice objavljene na internetskim stranicama Odbora.

91. Čak i ako se postupku obrade dodijeli certifikat u skladu s člankom 42., voditelj obrade i dalje je odgovoran za kontinuirano praćenje i poboljšanje usklađenosti s kriterijima tehničke i integrirane zaštite podataka iz članka 25.

[41] Vidjeti uvodnu izjavu 74. u skladu s kojom voditelji obrade moraju dokazati djelotvornost svojih mjera.
[42] Europski odbor za zaštitu podataka. „Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe". Verzija 3.0, 4. lipnja 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hr.pdf

5 PROVEDBA ČLANKA 25. I POSLJEDICE

92. Nadzorna tijela mogu procijeniti usklađenost s člankom 25. u skladu s postupcima navedenima u članku 58. Korektivne ovlasti navedene su u članku 58. stavku 2. i uključuju izdavanje upozorenja, službenih opomena, naloga za poštovanje prava ispitanika, ograničenja ili zabrane obrade, upravne novčane kazne itd.

93. Dodatni čimbenik u određivanju iznosa novčanih kazni za povrede Opće uredbe o zaštiti podataka jest tehnička i integrirana zaštita podataka; vidjeti članak 83. stavak 4.[43] [44]

6 PREPORUKE

94. Iako se ne spominju izravno u članku 25., izvršitelji obrade i proizvođači smatraju se ključnima za omogućavanje tehničke i integrirane zaštite podataka te bi trebali biti svjesni da voditelji obrade moraju samo obraditi osobne podatke s pomoću sustava i tehnologija u koje su ugrađeni elementi zaštite podataka.

95. Kad obrađuju podatke u ime voditelja obrade ili stavljaju na raspolaganje rješenja voditeljima obrade, izvršitelji obrade i proizvođači trebali bi primijeniti svoje znanje i iskustvo kako bi izgradili povjerenje i usmjerili svoje klijente, uključujući MSP-ove, pri izradi/nabavi rješenja kojima se zaštita podataka uključuje u obradu. To pak znači da bi se izradom proizvoda i usluga trebalo olakšati ispunjavanje potreba voditelja obrade.

96. Pri provedbi članka 25. trebalo bi imati na umu da je glavni cilj izrade *učinkovita provedba* načela i *zaštita* prava ispitanika u okviru odgovarajućih mjera obrade. Kako bi se olakšala i poboljšala provedba načela tehničke i integrirane zaštite podataka, voditeljima obrade te izvršiteljima obrade i proizvođačima dajemo sljedeće preporuke:
    - Voditelji obrade trebali bi uzeti u obzir zaštitu podataka od *početnih faza* planiranja obrade, čak i prije utvrđivanja načina obrade.
    - Ako voditelj obrade ima svojeg službenika za zaštitu podataka, Europski odbor za zaštitu podataka potiče aktivno sudjelovanje tog službenika u uključivanju tehničke i integrirane zaštite podataka u postupke nabave i izrade te u cijeli životni ciklus obrade.
    - Postupak obrade može se *certificirati*. Zahvaljujući mogućnosti certificiranja postupka obrade, voditelju obrade pruža se dodana vrijednost kada odabire različite vrste softvera, hardvera, usluga i/ili sustava za obradu od proizvođača ili izvršitelja obrade. Stoga bi proizvođači tijekom životnog ciklusa izrade rješenja za obradu trebali nastojati dokazati da postoji tehnička i integrirana zaštita podataka. Certifikacijski pečat može služiti i kao smjernica ispitanicima za odabir različitih proizvoda i usluga. Zahvaljujući mogućnosti certificiranja postupka obrade proizvođači, izvršitelji obrade i voditelji obrade mogu ostvariti konkurentsku prednost, a može se povećati i povjerenje ispitanika u obradu njihovih osobnih podataka. Ako ne postoji mogućnost certificiranja, voditelji obrade trebali bi pokušati pronaći druga *jamstva* da

[43] Člankom 83. stavkom 2. točkom (d) Opće uredbe o zaštiti podataka propisuje se da se pri utvrđivanju izricanja novčanih kazni za kršenje Opće uredbe o zaštiti podataka „dužna pozornost" posvećuje „stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s člancima 25. i 32.".

[44] Više informacija o kaznama može se pronaći u dokumentu Radne skupine iz članka 29. „Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679". WP 253, 3. listopada 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – potvrdio Europski odbor za zaštitu podataka

proizvođači ili izvršitelji obrade ispunjavaju zahtjeve u pogledu tehničke i integrirane zaštite podataka.

- Voditelji obrade, izvršitelji obrade i proizvođači trebali bi razmotriti svoju obvezu u pogledu toga da djeci mlađoj od 18 godina i drugim ranjivim skupinama osiguraju posebnu zaštitu u skladu s načelima tehničke i integrirane zaštite podataka.
- Proizvođači i izvršitelji obrade trebali bi nastojati olakšati provedbu načela tehničke i integrirane zaštite podataka kako bi se poduprla sposobnost voditelja obrade za ispunjavanje obveza iz članka 25. S druge strane, voditelji obrade ne bi trebali odabrati proizvođače ili izvršitelje obrade koji ne nude sustave koji voditeljima obrade omogućuju usklađivanje s člankom 25. ili im u tome pomažu, s obzirom na to da će se voditelje obrade smatrati odgovornima ako se tehnička i integrirana zaštita podataka ne provedu.
- Proizvođači i izvršitelji obrade trebali bi imati aktivnu ulogu u osiguravanju da su ispunjeni kriteriji za „najnovija dostignuća" i trebali bi voditelje obrade obavijestiti o svim promjenama u „najnovijim dostignućima" koje bi mogle utjecati na učinkovitost mjera koje oni provode. Voditelji obrade trebali bi taj zahtjev uključiti kao ugovornu odredbu kako bi osigurali da ih se doista obavještava o najnovijim promjenama.
- Europski odbor za zaštitu podataka preporučuje voditeljima obrade da od proizvođača i izvršitelja obrade zahtijevaju da pokažu na koji način njihovi hardver, softver, usluge ili sustavi omogućuju voditelju obrade da ispuni zahtjeve u pogledu odgovornosti u skladu s tehničkom i integriranom zaštitom podataka, na primjer, tako da upotrijebe ključne pokazatelje uspješnosti kako bi dokazali učinkovitost mjera i zaštitnih mjera pri provedbi načela i prava.
- Europski odbor za zaštitu podataka ističe potrebu za usklađenim pristupom učinkovitoj provedbi načela i prava te potiče udruženja ili tijela koja izrađuju kodekse ponašanja u skladu s člankom 40. da u njih uvrste i smjernice o tehničkoj i integriranoj zaštiti podataka za pojedine sektore.
- Voditelji obrade trebali bi biti pošteni prema ispitanicima i transparentno ocjenjivati i dokazivati učinkovitu provedbu tehničke i integrirane zaštite podataka, na isti način na koji voditelji obrade dokazuju usklađenost s Općom uredbom o zaštiti podataka u skladu s načelom odgovornosti.
- Ako je to primjereno u okviru pristupa temeljenog na riziku, kao mjera u skladu sa zahtjevima u pogledu tehničke i integrirane zaštite podataka mogu se upotrebljavati najnovije tehnologije za unapređenje zaštite privatnosti na visokom stupnju razvoja. Takvim tehnologijama samima po sebi nisu nužno obuhvaćene obveze iz članka 25. Voditelji obrade moraju procijeniti je li određena mjera primjerena i učinkovita za provedbu načela zaštite podataka i prava ispitanika.
- Postojeći naslijeđeni sustavi obuhvaćeni su istim obvezama u pogledu tehničke i integrirane zaštite podataka kao i novi sustavi. Ako naslijeđeni sustavi već nisu usklađeni s obvezama u pogledu tehničke i integrirane zaštite podataka i ne mogu se izvršiti promjene kako bi se ispunile te obveze, naslijeđeni sustavi jednostavno nisu usklađeni s obvezama iz Opće uredbe o zaštiti podataka i ne mogu se upotrebljavati za obradu osobnih podataka.
- Člankom 25. ne snižava se prag u pogledu zahtjeva za MSP-ove. Sljedeći savjeti mogu MSP-ovima olakšati usklađivanje s člankom 25.:
    - rano provedite procjene rizika
    - najprije obrađujte male količine podataka, a zatim postupno povećavajte njihov opseg i složenost

- potražite jamstva proizvođača i izvršitelja obrade u pogledu tehničke i integrirane zaštite podataka, kao što su certifikati i pridržavanje kodeksa ponašanja
- surađujte s partnerima koji ostvaruju dobre rezultate
- razgovarajte s tijelom za zaštitu podataka
- pročitajte smjernice tijela za zaštitu podataka i Europskog odbora za zaštitu podataka
- pridržavajte se kodeksa ponašanja ako su dostupni
- zatražite pomoć i savjet stručnjaka.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)