Suunised

Artiklit 25 käsitlevad suunised 4/2019

Lõimitud andmekaitse ja vaikimisi andmekaitse

Versioon 2.0.

Vastu võetud 20. oktoobril 2020

Versiooniajalugu

Versioon 1.0.	13. november 2019	Suuniste vastuvõtmine avalikuks konsulteerimiseks
Versioon 2.0.	20. oktoober 2020	Suuniste vastuvõtmine Euroopa Andmekaitsenõukogus pärast avalikku konsultatsiooni

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse 2016/679/EL (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi „isikuandmete kaitse üldmäärus“)) artikli 70 lõike 1 punkti e,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018,

võttes arvesse kodukorra artikleid 12 ja 22,

ON VASTU VÕTNUD JÄRGMISED SUUNISED:

Kommenteeritud kokkuvõte

Üha digitaalsemas maailmas on lõimitud andmekaitse ja vaikimisi andmekaitse nõuete järgimisel otsustav tähtsus ühiskonnas eraelu puutumatuse ja andmekaitse edendamisel. Seetõttu on oluline, et vastutavad töötlejad võtaksid seda kohust tõsiselt ja täidaksid töötlemistoimingute kavandamisel isikuandmete kaitse üldmäärusega kehtestatud kohustusi.

Käesolevas dokumendis antakse üldisi suuniseid isikuandmete kaitse üldmääruse artiklis 25 sätestatud lõimitud andmekaitse ja vaikimisi andmekaitse kohustuse kohta. Lõimitud ja vaikimisi andmekaitse kohustus kehtib kõigile vastutavatele töötlejatele, olenemata nende suurusest ja töötlemistoimingu keerukusest. Lõimitud ja vaikimisi andmekaitse nõuete täitmiseks on oluline, et vastutav töötleja mõistaks andmekaitsepõhimõtteid ning andmesubjekti õigusi ja vabadusi.

Peamine kohustus on rakendada *asjakohaseid* meetmeid ja vajalikke kaitsemeetmeid, millega tagatakse *andmekaitsepõhimõtete tõhus rakendamine* ning sellest tulenevalt *andmesubjektide õiguste ja vabaduste lõimitud ja vaikimisi kaitse*. Artiklis 25 on sätestatud nii lõimitud kui ka vaikimisi andmekaitse aspektid, mida tuleb arvesse võtta. Neid aspekte käsitletakse üksikasjalikumalt käesolevates suunistes.

Artikli 25 lõikes 1 on sätestatud, et vastutavatel töötlejatel tuleb uue töötlemistoimingu kavandamisel juba varakult silmas pidada lõimitud ja vaikimisi andmekaitset. Vastutavad töötlejad rakendavad lõimitud ja vaikimisi andmekaitset nii *enne* töötlemist kui ka *pidevalt* töötlemise ajal, vaadates korrapäraselt läbi valitud meetmete ja kaitsemeetmete tõhususe. Lõimitud ja vaikimisi andmekaitse kohustus kehtib ka olemasolevate süsteemide suhtes, milles töödeldakse isikuandmeid.

Ühtlasi sisaldavad käesolevad suunised juhtnööre, kuidas tõhusalt rakendada artiklis 5 sätestatud andmekaitsepõhimõtteid, ning siin on esitatud peamised lõimitud ja vaikimisi andmekaitse aspektid ning toodud praktilisi näiteid. Vastutav töötleja peaks kaaluma soovitatud meetmete asjakohasust kindla töötlemistoimingu puhul.

Euroopa Andmekaitsenõukogu annab soovitusi selle kohta, kuidas vastutavad töötlejad, volitatud töötlejad ja tootjad saavad teha koostööd lõimitud ja vaikimisi andmekaitse tagamiseks. Andmekaitsenõukogu innustab tööstusvaldkonna vastutavaid töötlejaid, volitatud töötlejaid ja tootjaid kasutama lõimitud ja vaikimisi andmekaitset konkurentsieelise saavutamiseks, kui nad

turustavad oma tooteid vastutavatele töötlejatele ja andmesubjektidele. Samuti innustatakse kõiki vastutavaid töötlejaid kasutama sertifitseerimist ja toimimisjuhendeid.

1 KOHALDAMISALA

1. Suunised keskenduvad lõimitud ja vaikimisi andmekaitse rakendamisele vastutavate töötlejate poolt, lähtudes isikuandmete kaitse üldmääruse artiklis 25 sätestatud kohustusest.[1] Muudele osapooltele, nagu volitatud töötlejad ning toodete, teenuste ja rakenduste tootjad (edaspidi „tootjad"), keda ei ole artiklis 25 otseselt käsitletud, võivad suunised samuti kasulikud olla, aidates luua isikuandmete kaitse üldmäärusele vastavaid tooteid ja teenuseid, mis võimaldavad vastutavatel töötlejatel täita andmekaitsekohustusi.[2] Isikuandmete kaitse üldmääruse põhjenduses 78 juhitakse tähelepanu sellele, et riigihangete kontekstis tuleb samuti võtta arvesse lõimitud andmekaitset ja vaikimisi andmekaitset. Kuigi kõigil vastutavatel töötlejatel on kohustus integreerida lõimitud ja vaikimisi andmekaitse oma töötlemistoimingutesse, edendab see säte andmekaitsepõhimõtete järgimist ning siinkohal peaksid eeskujuks olema riiklikud haldusasutused. Vastutav töötleja vastutab selle eest, et tema volitatud töötlejate ja alamtöötlejate töötlemistoimingute puhul täidetaks lõimitud ja vaikimisi andmekaitse kohustusi, ning ta peaks seda nende pooltega lepingute sõlmimisel arvesse võtma.

2. Artiklis 25 kirjeldatud nõue seisneb selles, et vastutavatel töötlejatel peab olema andmekaitse vaikimisi isikuandmete töötlemisse lõimitud, ja see kehtib kogu töötlemisprotsessi suhtes. Lõimitud ja vaikimisi andmekaitse nõue kehtib ka töötlemissüsteemide suhtes, mis olid olemas juba enne isikuandmete kaitse üldmääruse jõustumist. Vastutavad töötlejad peavad töötlemistoiminguid kooskõlas isikuandmete kaitse üldmäärusega pidevalt ajakohastama. Lisateavet selle kohta, kuidas tagada, et olemasolev süsteem oleks kooskõlas lõimitud ja vaikimisi andmekaitse põhimõtetega, leiate käesolevate suuniste jaotisest 2.1.4. Sätte põhieesmärk on tagada *asjakohane* ja *tõhus lõimitud* andmekaitse ja *vaikimisi* andmekaitse, mis tähendab, et vastutavad töötlejad peavad suutma tõendada, et nad kohaldavad töötlemisel asjakohaseid meetmeid ja kaitsemeetmeid, millega kindlustatakse andmekaitsepõhimõtetest ning andmesubjektide õigustest ja vabadustest kinnipidamine.

3. Suuniste 2. peatükis on tõlgendatud artikliga 25 kehtestatud nõudeid ja käsitletud sättest tulenevaid juriidilisi kohustusi. 3. peatükis on toodud näiteid selle kohta, kuidas rakendada lõimitud ja vaikimisi andmekaitset konkreetsete andmekaitsepõhimõtete kontekstis.

4. Suuniste 4. peatükis käsitletakse võimalust luua sertifitseerimismehhanism artiklile 25 vastavuse tõendamiseks ja 5. peatükis räägitakse sellest, kuidas järelevalveasutused saavad artiklit jõustada. Samuti antakse suunistes sidusrühmadele soovitusi, kuidas lõimitud ja vaikimisi andmekaitset edukalt rakendada. Euroopa Andmekaitsenõukogu tõdeb, et väikestel ja keskmise suurusega ettevõtjatel

[1] Siin esitatud tõlgendusi kohaldatakse samaväärselt direktiivi (EL) 2016/680 artiklile 20 ja määruse (EL) 2018/1725 artiklile 27.

[2] Isikuandmete kaitse üldmääruse põhjenduses 78 on sellele vajadusele selgelt tähelepanu juhitud: „Selliste rakenduste, teenuste ja toodete väljatöötamisel, kavandamisel, valimisel ja kasutamisel, mis põhinevad isikuandmete töötlemisel või mille käigus töödeldakse isikuandmeid nende ülesannete täitmiseks, tuleks nende toodete, teenuste ja rakenduste tootjaid innustada võtma selliste toodete, teenuste ja rakenduste väljatöötamisel ja kavandamisel arvesse õigust andmekaitsele ning tagama asjakohaselt teaduse ja tehnoloogia viimast arengut arvestades, et vastutavad töötlejad ja volitatud töötlejad saaksid täita oma andmekaitsealaseid kohustusi".

(edaspidi „VKEd“) võib olla keeruline lõimitud ja vaikimisi andmekaitse kohustusi täielikult täita, ning esitab 6. peatükis just VKEdele mõeldud lisasoovitused.

2 ARTIKLI 25 („LÕIMITUD ANDMEKAITSE JA VAIKIMISI ANDMEKAITSE“) LÕIGETE 1 JA 2 ANALÜÜS

5. Käesoleva peatüki eesmärk on anda selgitusi ja suuniseid vastavalt artikli 25 lõikes 1 esitatud lõimitud andmekaitse nõuete ja artikli 25 lõikes 2 esitatud vaikimisi andmekaitse nõuete kohta. Lõimitud andmekaitse ja vaikimisi andmekaitse on teineteist vastastikku täiendavad ja toetavad mõisted. Andmesubjektid saavad vaikimisi andmekaitsest rohkem kasu, kui samal ajal rakendatakse lõimitud andmekaitset – ja vastupidi.

6. Lõimitud andmekaitse ja vaikimisi andmekaitse nõue kehtib kõigile vastutavatele töötlejatele, sealhulgas nii väikeettevõtjatele kui ka suurtele rahvusvahelistele ettevõtetele. Seega võib lõimitud ja vaikimisi andmekaitse rakendamine olla eri töötlemistoimingute puhul erineva keerukusega. Olenemata organisatsiooni suurusest toob lõimitud ja vaikimisi andmekaitse rakendamine vastutavale töötlejale ja andmesubjektile igal juhul kasu.

2.1 Artikli 25 lõige 1: lõimitud andmekaitse

2.1.1 Vastutava töötleja kohustus rakendada töötlemisel asjakohaseid tehnilisi ja korralduslikke meetmeid ning vajalikke kaitsemeetmeid

7. Artikli 25 lõike 1 kohaselt peab vastutav töötleja rakendama *asjakohaseid* tehnilisi ja korralduslikke *meetmeid,* mis on vajalikud andmekaitsepõhimõtete rakendamiseks, ning lõimima töötlemisse *vajalikud kaitsemeetmed*, et täita määruse nõudeid ning kaitsta andmesubjektide õigusi ja vabadusi. Nii asjakohased meetmed kui ka vajalikud kaitsemeetmed täidavad sama eesmärki, st kaitsevad andmesubjektide õigusi ja tagavad, et isikuandmete kaitse on töötlemise lahutamatu osa.

8. Mõisteid *tehnilised ja korralduslikud meetmed* ning *vajalikud kaitsemeetmed* kasutatakse laias tähenduses – need on mis tahes meetodid või vahendid, mida vastutav töötleja võib töötlemisel kasutada. *Asjakohasuse* all peetakse silmas, et meetmed ja vajalikud kaitsemeetmed peavad sobima kavandatud eesmärgi saavutamiseks, st need peavad tagama andmekaitsepõhimõtete *tõhusa* rakendamise[3]. Asjakohasuse nõue on seega tihedalt seotud tõhususe nõudega.

9. Tehniline või korralduslik meede ja kaitsemeede võib olla milline tahes, alates tipptasemel tehnilistest lahendustest ja lõpetades töötajate baaskoolitusega. Sõltuvalt asjaomase töötlemise kontekstist ja sellega seotud ohtudest võivad sobivad meetmed olla näiteks isikuandmete pseudonüümimine;[4] kättesaadavate isikuandmete säilitamine struktureeritud, üldiselt masinloetavas vormingus; andmesubjektidele töötlemisse sekkumise võimaldamine; teabe andmine isikuandmete säilitamise kohta; pahavara tuvastamise süsteemide kasutamine; töötajate koolitamine elementaarse küberhügieeni teemal; eraelu puutumatuse ja infoturbe haldamise süsteemide kasutuselevõtmine; volitatud töötlejate lepinguline kohustus rakendada kindlaid võimalikult väheste andmete kogumise tavasid jne.

[3] Mõistet „tõhusus“ on käsitletud allpool jaotises 2.1.2.
[4] Määratletud isikuandmete kaitse üldmääruse artikli 4 punktis 5.

10. Asjakohaste meetmete kindlaksmääramisel võivad abiks olla standardid, parimad tavad ja toimimisjuhendid, mida tunnustavad ühingud ja muud vastutavate töötlejate kategooriaid esindavad organid. Vastutav töötleja peab siiski kontrollima meetmete asjakohasust konkreetse töötlemistoimingu puhul.

2.1.2 Kavandatud andmekaitsepõhimõtete tõhusaks rakendamiseks ning andmesubjektide õiguste ja vabaduste kaitseks

11. *Andmekaitsepõhimõtted* on sätestatud artiklis 5 (edaspidi „põhimõtted“) ning *andmesubjektide õigused ja vabadused* on füüsiliste isikute põhiõigused ja -vabadused (eelkõige nende õigus isikuandmete kaitsele), mille kaitse on ette nähtud isikuandmete kaitse üldmääruse artikli 1 lõikega 2 (edaspidi „õigused“)[5]. Nende täpne sõnastus on esitatud Euroopa Liidu põhiõiguste hartas. On oluline, et vastutav töötleja mõistaks *põhimõtete* ja *õiguste* tähendust, sest sellel põhineb isikuandmete kaitse üldmäärusega ning eelkõige lõimitud ja vaikimisi andmekaitse kohustusega tagatav kaitse.

12. Asjakohaste tehniliste ja korralduslike meetmete rakendamisel tuleb meetmed ja kaitsemeetmed *kavandada* iga eespool nimetatud põhimõtte tõhusat rakendamist ja sellega kaasnevat õiguste kaitset silmas pidades.

Tõhususe käsitlus

13. Lõimitud andmekaitse keskmes on tõhusus. Põhimõtete tõhusa rakendamise nõue tähendab, et vastutavad töötlejad peavad rakendama nende põhimõtete kaitsmiseks vajalikke meetmeid ja kaitsemeetmeid, et tagada andmesubjektide õigused. Iga rakendatud meede peaks võimaldama saavutada vastutava töötleja ettenähtud töötlemistoimingu kavandatud tulemused. Sellest lähtub kaks asjaolu.

14. Esiteks tähendab see, et artikliga 25 ei nõuta kindlate tehniliste ega korralduslike meetmete rakendamist, vaid et valitud meetmed ja kaitsemeetmed peaksid tagama andmekaitsepõhimõtete rakendamise just selle konkreetse töötlemistoimingu puhul. Seejuures tuleks meetmed ja kaitsemeetmed kavandada nii, et need oleksid töökindlad, ning vastutaval töötlejal peaks olema võimalik rakendada lisameetmeid, et võtta arvesse riski suurenemist[6]. See, kas meetmed on tõhusad või mitte, oleneb seega asjaomase töötlemistoimingu kontekstist ning teatavate aspektide hindamisest, mida tuleb töötlemisvahendite kindlaksmääramisel arvesse võtta. Eespool nimetatud aspekte käsitletakse allpool jaotises 2.1.3.

15. Teiseks peaksid vastutavad töötlejad suutma tõendada, et põhimõtteid on järgitud.

16. Rakendatavad meetmed ja kaitsemeetmed peaksid saavutama andmekaitse seisukohast soovitud mõju ning vastutav töötleja peaks sellised meetmed dokumenteerima[7]. Selleks võib vastutav töötleja kindlaks määrata asjakohased tulemuslikkuse põhinäitajad, millega tõhusust tõendada. Tulemuslikkuse põhinäitaja on vastutava töötleja valitud mõõdetav väärtus, mis näitab, kui tõhusalt

[5] Vt isikuandmete kaitse üldmääruse põhjendus 4.

[6] Vastutavatele töötlejatele kohaldatavad aluspõhimõtted (s.o seaduslikkus, võimalikult väheste andmete kogumine, eesmärgi piirang, läbipaistvus, andmeterviklus, andmete õigsus) peavad jääma samaks, olenemata töötlemisest ja ohtudest andmesubjektidele. Sellise töötlemise laadi ja ulatust on aga nende põhimõtete rakendamisel alati nõuetekohaselt arvesse võetud, nii et need on oma olemuselt laiendatavad. Artikli 29 töörühm. „Statement on the role of a risk-based approach in data protection legal frameworks“ (Avaldus andmekaitse õigusraamistikes riskipõhise käsitluse otstarbe kohta). WP 218, 30. mai 2014, lk 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Vt põhjendused 74 ja 78.

vastutav töötleja täidab oma andmekaitse-eesmärki. Tulemuslikkuse põhinäitajad võivad olla *kvantitatiivsed* (näiteks valepositiivsete või valenegatiivsete tulemuste osakaal, kaebuste arvu vähendamine, vastamisaja vähendamine, kui andmesubjektid kasutavad oma õigusi) või *kvalitatiivsed* (näiteks tulemuslikkuse hindamine, hindamisskaala kasutamine või eksperdihinnangud). Tulemuslikkuse põhinäitajate asemel võivad vastutavad töötlejad tõendada põhimõtete tõhusat rakendamist ka sel teel, et nad esitavad põhjused, millel põhineb nende hinnang valitud meetmete ja kaitsemeetmete tõhususele.

2.1.3 Aspektid, mida tuleb arvesse võtta

17. Artikli 25 lõikes 1 on loetletud aspektid, mida vastutav töötleja peab konkreetse töötlemistoimingu meetmete kindlaksmääramisel arvesse võtma. Järgnevalt on esitatud suunised, kuidas neid aspekte kavandamisprotsessis silmas pidada, sh vaikeseadete kavandamisel. Kõik need aspektid aitavad kindlaks teha, kas meede on põhimõtete tõhusaks rakendamiseks asjakohane. Seega ei ole kõik need aspektid omaette eesmärk, vaid neid tuleb eesmärgi saavutamiseks käsitleda koos.

2.1.3.1 Teaduse ja tehnoloogia viimane areng

18. Mõistet „teaduse ja tehnoloogia viimane areng“ kasutatakse mitmes ELi õigustikus, nt keskkonnakaitse ja tooteohutuse vallas. Isikuandmete kaitse üldmääruses viidatakse „teaduse ja tehnoloogia viimasele arengule“[8] mitte ainult artiklis 32 seoses turbemeetmetega,[9][10] vaid ka artiklis 25, laiendades nii seda võrdlusalust kõikidele tehnilistele ja korralduslikele meetmetele, mida töötlemine hõlmab.

19. Artikli 25 kontekstis kehtestatakse teaduse ja tehnoloogia viimasele arengule viitamisega vastutavatele töötlejatele kohustus, et asjakohaste tehniliste ja korralduslike meetmete kindlaksmääramisel tuleb **arvesse võtta tänapäevast arengut tehnoloogias**, mis on turul saadaval. Vastutavatel töötlejatel peavad olema teadmised tehnoloogia edusammudest; sellest, kuidas tehnoloogiaga võivad kaasneda andmekaitseohud töötlemistoimingule ja ka võimalused, ning sellest, kuidas rakendada ja ajakohastada meetmeid ja kaitsemeetmeid, mis tagavad muutuval tehnoloogiamaastikul põhimõtete ja andmesubjektide õiguste *tõhusa rakendamise*, ning nad peavad hoidma ennast nendega kursis.

20. „Teaduse ja tehnoloogia viimane areng“ on dünaamiline mõiste, mida ei ole võimalik määratleda staatiliselt kindlal ajahetkel, vaid seda tuleks tehnoloogia arengu kontekstis *pidevalt* hinnata. Tehnoloogia saavutuste taustal võib vastutav töötleja leida, et meede, mis kunagi tagas piisava kaitse, ei ole enam piisav. Kui tehnoloogia muudatustega ei peeta sammu, võib selle tulemus olla artikli 25 rikkumine.

21. Teaduse ja tehnoloogia viimase arengu kriteeriumi ei kohaldata mitte ainult tehnilistele meetmetele, vaid ka korralduslikele meetmetele. Asjakohaste korralduslike meetmete puudumine võib vähendada valitud tehnoloogia tõhusust või selle isegi olematuks muuta. Korralduslikud meetmed võivad olla

[8] Vt Saksamaa Föderaalse Konstitutsioonikohtu 1978. aasta otsust Kalkari kohtuasjas (https://germanlawarchive.iuscomp.org/?p=67), mis võib anda aluse mõiste objektiivse määratlemise metoodikale. Selle põhjal võib öelda, et „teaduse ja tehnoloogia viimasele arengule“ vastav tehnoloogia tase jääb „olemasolevatel teaduslikel andmetel ja uuringutel“ põhineva tehnoloogia taseme ning väljakujunenud „üldtunnustatud tehnoloogiaeeskirjade“ vahele. Seega võib teaduse ja tehnoloogia viimast arengut määratleda turul saadaoleva teenuse või tehnika või toote tehnoloogia tasemena, mis on määratletud eesmärkide täitmiseks kõige tõhusam.

[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/.

näiteks sisepoliitika vastuvõtmine, ajakohane tehnoloogia-, turbe- ja andmekaitsealane koolitus ning IT-turbe juhtimise ja haldamise poliitika.

22. Eri valdkondades kehtivad tunnustatud raamistikud, standardid, sertifitseerimine, tegevusjuhendid jne võivad anda ettekujutuse praegusest teaduse ja tehnika tasemest asjaomases valdkonnas. Kui sellised standardid on olemas ja tagavad andmesubjektile kõrgetasemelise kaitse kooskõlas õigusnõuetega – või neid isegi ületades –, peaksid vastutavad töötlejad neid andmekaitsemeetmete kavandamisel ja rakendamisel arvesse võtma.

2.1.3.2 Rakendamise kulud

23. Kui vastutav töötleja valib ja kohaldab asjakohaseid tehnilisi ja korralduslikke meetmeid ning vajalikke kaitsemeetmeid, et andmesubjektide õiguste kaitsmiseks tõhusalt rakendada andmekaitsepõhimõtteid, võib ta arvesse võtta rakendamise kulusid. Kulud viitavad ressurssidele üldiselt, sh ajale ja töötajatele.

24. Kulusättega ei nõuta, et vastutav töötleja kulutaks ebaproportsionaalselt palju ressursse, kui on olemas alternatiivsed meetmed, mille jaoks kulub vähem ressursse, kuid mis on endiselt tõhusad. Siiski on rakendamiskulud tegur, mida tuleb arvesse võtta lõimitud andmekaitse rakendamisel, mitte põhjus, miks seda ei rakendata.

25. Seega peavad valitud meetmed tagama, et vastutav töötleja ei riku isikuandmeid töödeldes andmekaitsepõhimõtteid, sõltumata kuludest. Vastutavad töötlejad peaksid suutma hallata üldkulusid, et tõhusalt rakendada kõiki põhimõtteid ja seega kaitsta õigusi.

2.1.3.3 Töötlemise laad, ulatus, kontekst ja eesmärk

26. Vastutavad töötlejad peavad vajalike meetmete kindlaksmääramisel võtma arvesse töötlemise laadi, ulatust, konteksti ja eesmärki.

27. Et lõimida andmekaitsepõhimõtted isikuandmete töötlemisse, tuleks neid tegureid tõlgendada kooskõlas nende rolliga isikuandmete kaitse üldmääruse muudes sätetes, näiteks artiklites 24, 32 ja 35.

28. Lühidalt võib **laadi** mõista kui töötlemisele omaseid[11] tunnuseid. **Ulatus** viitab töötlemise mahule ja piiridele. **Kontekst** on seotud töötlemise asjaoludega, mis võivad mõjutada andmesubjekti ootusi, ning **eesmärk** hõlmab töötlemise eesmärke.

2.1.3.4 Töötlemisest tulenevad füüsiliste isikute õigusi ja vabadusi ähvardavad erineva tõenäosuse ja suurusega ohud

29. Isikuandmete kaitse üldmääruse artiklite 24, 25, 32 ja 35 paljudes sätetes rakendatakse sidusat riskipõhist lähenemisviisi, mis aitab kindlaks määrata asjakohased tehnilised ja korralduslikud meetmed, et kaitsta üksikisikuid ja nende isikuandmeid ning täita isikuandmete kaitse üldmääruse nõudeid. Kaitstav vara on alati sama (üksikisikud, nende isikuandmete kaitsmise kaudu) ning kaitstakse samade ohtude vastu (ohud üksikisikute õigustele), võttes arvesse samu tingimusi (töötlemise laad, ulatus, kontekst ja eesmärk).

[11] Näiteks isikuandmete eriliigid, automaatne otsuste tegemine, kallutatud võimusuhted, ettearvamatu töötlemine, andmesubjekti raskused õiguste kasutamisel jne.

30. Artikli 25 järgimise kohta riskianalüüsi tehes peab vastutav töötleja kindlaks tegema andmekaitsepõhimõtete rikkumisest tulenevad ohud andmesubjektide õigustele ning välja selgitama nende ohtude tõenäosuse ja tõsiduse, et rakendada meetmeid tuvastatud riskide tõhusaks leevendamiseks. Riskihindamisel on väga oluline töötlemistoimingut süstemaatiliselt ja põhjalikult hinnata. Näiteks hindab vastutav töötleja konkreetseid riske seoses vabatahtliku nõusoleku puudumisega, mis kujutab endast seaduslikkuse põhimõtte rikkumist alla 18-aastaste laste ja noorte kui haavatava rühma isikuandmete töötlemise puhul, kui puudub muu õiguslik alus, ning rakendab asjakohaseid meetmeid, et käsitleda ja tõhusalt leevendada tuvastatud riske, mis on seotud selle andmesubjektide rühmaga.

31. Euroopa Andmekaitsenõukogu suunistes, mis käsitlevad andmekaitsealast mõjuhinnangut[12] ning selle kindlaksmääramist, kas töötlemistoimingu tulemusena tekib andmesubjektile tõenäoliselt suur oht või mitte, antakse juhtnööre ka selle kohta, kuidas hinnata andmekaitseohte ja läbi viia andmekaitsealast riskihindamist. Suunistest võib olla abi ka kõikide eespool nimetatud artiklite, sh artikliga 25 seotud riskihindamisel.

32. Riskipõhine käsitlus ei välista lähtetasemete, parimate tavade ja standardite kasutamist. Need võivad olla kasulikud vahendid, mida vastutavad töötlejad saaksid kasutada sarnastes olukordades sarnaste ohtude ohjamisel (töötlemise laad, ulatus, kontekst ja eesmärk). Siiski jääb kehtima artiklis 25 (ning artiklites 24, 32 ja artikli 35 lõike 7 punktis c sätestatud kohustus võtta arvesse „töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte“. Seetõttu peavad vastutavad töötlejad, ehkki neile on abiks sellised vahendid, alati igal üksikjuhul eraldi hindama töötlemistoimingust tulenevaid ohte andmekaitsele ning kontrollima kavandatavate meetmete ja kaitsemeetmete tõhusust. Sellisel juhul võib olla vajalik ka andmekaitsealane mõjuhinnang või olemasoleva andmekaitsealase mõjuhinnangu ajakohastamine.

2.1.4 Ajaline aspekt

2.1.4.1 Töötlemisvahendite kindlaksmääramise ajal

33. Lõimitud andmekaitset tuleb rakendada *töötlemisvahendite kindlaksmääramisel*.

34. *Töötlemisvahendid* võivad olla mitmesugused, alates töötlemise üldistest aspektidest ja lõpetades üksikasjalike aspektidega, näiteks arhitektuur, menetlused, protokollid, kujundus ja välisilme.

35. *Töötlemisvahendite kindlaksmääramise aeg* viitab ajavahemikule, mille jooksul vastutav töötleja otsustab, kuidas töötlemine toimub ning millised on töötlemisviisid ja töötlemiseks kasutatavad mehhanismid. Selliste otsuste langetamise käigus peab vastutav töötleja hindama asjakohaseid meetmeid ja kaitsemeetmeid, et andmekaitsepõhimõtteid ja andmesubjektide õigusi töötlemisprotsessis tõhusalt arvesse võtta, ning pidama silmas selliseid aspekte nagu teaduse ja tehnoloogia viimane areng, rakendamiskulud, laad, ulatus, kontekst ja eesmärk ning ohud. See hõlmab andmetöötlustarkvara, -riistvara ja -teenuste hankimise ja rakendamise aega.

36. Lõimitud ja vaikimisi andmekaitsele on oluline juba varakult tähelepanu pöörata, et põhimõtteid edukalt rakendada ja kaitsta andmesubjektide õigusi. Kulutasuvuse seisukohast on vastutavate

[12] Artikli 29 töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679. WP 248 rev.01, 4. oktoober 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 – kinnitanud Euroopa Andmekaitsenõukogu.

töötlejate huvides võtta seda arvesse pigem varem kui hiljem, kuna juba tehtud plaanidesse ja kavandatud töötlemistoimingutesse hilisemate muudatuste tegemine võib olla probleemne ja kulukas.

2.1.4.2 Töötlemise ajal (andmekaitsenõuete rakendamine ja läbivaatamine)

37. Kui töötlemine on alanud, on vastutaval töötlejal jätkuvalt kohustus säilitada lõimitud ja vaikimisi andmekaitse, st põhimõtete jätkuv tõhus rakendamine, et kaitsta õigusi, ajakohastades tehnika taset, hinnates uuesti ohu taset jne. Töötlemistoimingute laad, ulatus ja kontekst ning ohud võivad töötlemise käigus muutuda, mis tähendab, et vastutav töötleja peab oma töötlemistoimingud korrapäraselt läbi vaatama ja hindama valitud meetmete ja kaitsemeetmete tõhusust.

38. Töötlemistoimingu nõuetele vastavana hoidmise, läbivaatamise ja vajaduse korral ajakohastamise kohustus kehtib ka olemasolevate süsteemide suhtes. See tähendab, et enne isikuandmete kaitse üldmääruse jõustumist loodud varasemad süsteemid tuleb läbi vaadata ja neid tuleb kohandada, et tagada selliste meetmete ja kaitsemeetmete kasutamine, millega rakendatakse tõhusalt andmekaitsepõhimõtteid ja andmesubjektide õigusi, nagu on kirjeldatud käesolevates suunistes.

39. See kohustus laieneb ka mis tahes töötlemistoimingutele, mida teevad volitatud töötlejad. Vastutavatel töötlejatel tuleb volitatud töötlejate toiminguid regulaarselt kontrollida ja hinnata, tagamaks, et need võimaldavad põhimõtteid pidevalt järgida ning vastutavatel töötlejatel oma vastavaid kohustusi täita.

2.2 Artikli 25 lõige 2: vaikimisi andmekaitse

2.2.1 Vaikimisi töödeldakse ainult isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks.

40. Mõiste „vaikimisi“, nagu seda tavaliselt informaatikas määratletakse, viitab eelnevalt olemasolevale või eelvalitud seadistuse väärtusele, mis on määratud tarkvararakendusele, arvutiprogrammile või seadmele. Selliseid seadistusi nimetatakse ka „eelseadistusteks“ või „tehase seadistusteks“, eelkõige elektroonikaseadmete puhul.

41. Seega viitab termin „vaikimisi“ isikuandmete töötlemisel valikute tegemisele seoses konfiguratsiooni väärtuste või töötlemisvõimalustega, mis on määratud või ette nähtud töötlemissüsteemis, nagu tarkvararakendus, teenus või seade või käsitsi töötlemine, mis mõjutab kogutavate isikuandmete hulka, nende töötlemise ulatust, säilitamise aega ja kättesaadavust.

42. Vastutav töötleja peaks valima niisugused töötlemise vaikeseaded ja -valikud, et vaikimisi toimuks ainult selline töötlemine, mis on tingimata vajalik seatud õiguspärase eesmärgi täitmiseks, ning vastutama nende rakendamise eest. Seejuures peavad vastutavad töötlejad tuginema oma hinnangule töötlemise vajalikkuse kohta, lähtudes artikli 6 lõikes 1 esitatud õiguslikest alustest. See tähendab, et vaikimisi ei kogu vastutav töötleja rohkem andmeid kui vaja, ei töötle kogutud andmeid rohkem, kui on vajalik tema eesmärkide saavutamiseks, ega säilita andmeid kauem kui vaja. Peamine nõue on, et töötlemine peab vaikimisi hõlmama andmekaitset.

43. Vastutav töötleja on kohustatud ette määrama, millistel täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel isikuandmeid kogutakse ja töödeldakse[13]. Meetmed peavad vaikimisi olema asjakohased, et töödeldaks vaid töötlemise iga konkreetse eesmärgi saavutamiseks vajalikke isikuandmeid. Euroopa Andmekaitseinspektori suunistest, mis käsitlevad isikuandmete kaitse õigust

[13] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktid b, c, d ja e.

piiravate meetmete vajalikkuse ja proportsionaalsuse hindamist, võib olla abi ka otsustamisel, milliseid andmeid on vaja konkreetse eesmärgi saavutamiseks töödelda[14] [15] [16].

44. Kui vastutav töötleja kasutab kolmanda isiku tarkvara või valmistarkvara, peaks ta tegema toote riskihindamise ja tagama, et funktsioonid, millel puudub õiguslik alus või mis ei ole kooskõlas töötlemise kavandatud eesmärgiga, on välja lülitatud.

45. Samad kaalutlused kehtivad töötlemistoiminguid toetavate korralduslike meetmete puhul. Need peaksid olema kavandatud nii, et alguses töödeldakse vaid minimaalne hulk konkreetsete toimingute jaoks vajalikke isikuandmeid. Seda tuleks eelkõige arvesse võtta andmetele juurdepääsu andmisel erineva ametipositsiooni ja juurdepääsuvajadusega töötajatele.

46. Terminit „asjakohased tehnilised ja korralduslikud meetmed“ mõistetakse vaikimisi andmekaitse kontekstis samamoodi, nagu on käsitletud eespool jaotises 2.1.1, kuid seda kasutatakse võimalikult väheste andmete kogumise põhimõtte rakendamisel.

47. Eespool nimetatud kohustust töödelda vaid iga konkreetse eesmärgi saavutamiseks vajalikke isikuandmeid kohaldatakse järgmiste aspektide suhtes.

2.2.2 Võimalikult väheste andmete kogumise kohustuse eri tahud

48. Artikli 25 lõikes 2 on nimetatud võimalikult väheste andmete kogumise kohustuse eri tahud: kohustus kehtib kogutud isikuandmete hulga, nende töötlemise ulatuse, säilitamise aja ja kättesaadavuse suhtes.

2.2.2.1 Kogutavate isikuandmete hulk

49. Vastutavad töötlejad peavad arvesse võtma nii töötlemise eesmärkide saavutamiseks vajalike isikuandmete hulka kui ka nende liike, kategooriaid ja üksikasjalikkust. Töötlemise kavandamisel tuleb arvesse võtta suures koguses üksikasjalike isikuandmete kogumisest tulenevaid suuremaid ohte tervikluse ja konfidentsiaalsuse, võimalikult väheste andmete kogumise ja andmete säilitamise piirangu põhimõttele ning võrrelda neid ohte väiksemate ohtudega, millega on võimalik piirduda, kui andmesubjektide kohta kogutakse vähem üksikasjalikku teavet. Igal juhul ei tohi vaikeseade hõlmata töötlemise konkreetse eesmärgi saavutamiseks ebavajalike isikuandmete kogumist. Teisisõnu, kui teatud isikuandmete liigid on ebavajalikud või kui üksikasjalikke andmeid ei ole vaja, kuna vähem üksikasjalikest andmetest piisab, siis liigseid isikuandmeid ei koguta.

50. Samad vaikenõuded kehtivad teenuste suhtes: olenemata kasutatavast platvormist või seadmest tohib koguda üksnes konkreetseks otstarbeks vajalikke isikuandmeid.

---

[14] Euroopa Andmekaitseinspektor, „EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data“ (Euroopa Andmekaitseinspektori suunised, et hinnata andmekaitse õiguse piiramise meetmete vajadust ja proportsionaalsust). 25. veebruar 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[15] Vt ka Euroopa Andmekaitseinspektori teabematerjali „Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data: A Toolkit” (Isikuandmete kaitse põhiõiguse piiramise meetmete vajaduse hindamise vahendid), https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[16] Lisateavet vajalikkuse kohta vt artikli 29 töörühma arvamusest 06/2014 andmete vastutava töötleja õigustatud huvide mõiste kohta direktiivi 95/46/EÜ artikli 7 tähenduses. WP 217, 9. aprill 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_et.pdf.

2.2.2.2 Isikuandmete töötlemise ulatus

51. Isikuandmete töötlemise[17] toimingud peavad piirduma sellega, mis on vajalik. Töötlemiseesmärki võivad aidata saavutada paljud töötlemistoimingud. See, et isikuandmed on eesmärgi saavutamiseks vajalikud, ei tähenda aga, et andmetega võib teha igat liiki ja igasuguse sagedusega töötlemistoiminguid. Vastutavad töötlejad peavad kandma hoolt ka selle eest, et ei laiendataks artikli 6 lõikes 4 sätestatud kooskõlas olevate eesmärkide piire, ning silmas pidama seda, milline töötlemine jääb andmesubjektide mõistlike eelduste piiridesse.

2.2.2.3 Isikuandmete säilitamise aeg

52. Kogutud isikuandmeid ei säilitata, kui need ei ole töötlemise eesmärgi saavutamiseks vajalikud ning puudub muu asjakohane eesmärk ja õiguslik alus, mis oleks kooskõlas artikli 6 lõikega 4. Vastutav töötleja peab suutma säilitamise vajalikkust kooskõlas vastutuse põhimõttega objektiivselt põhjendada.

53. Vastutav töötleja säilitab andmeid ainult niikaua, kui see on vajalik eesmärgi täitmiseks. Kui isikuandmeid ei ole nende töötlemise eesmärgil enam vaja, tuleb need vaikimisi kustutada või anonüümseks muuta. Seega sõltub säilitamisperioodi pikkus asjaomase töötlemise eesmärgist. See kohustus on otseselt seotud artikli 5 lõike 1 punktis e sätestatud säilitamise piirangu põhimõttega ning seda tuleb rakendada vaikimisi, s.o vastutava töötleja töötlemistoimingute juurde peavad kuuluma süstemaatilised menetlused andmete kustutamiseks või anonüümimiseks.

54. Isikuandmete anonüümseks muutmine[18] on alternatiiv kustutamisele, tingimusel et arvesse võetakse kogu asjakohast konteksti ning regulaarselt hinnatakse ohtude, sh taasidentifitseerimise ohu tõenäosust ja suurust[19].

2.2.2.4 Isikuandmete kättesaadavus

55. Vastutav töötleja peab vajalikkuse hindamise alusel piirama seda, kes ja kuidas isikuandmetele ligi pääseb, ning ühtlasi tagama, et isikuandmetele pääsevad ligi inimesed, kellel on seda vaja, näiteks kriitilistes olukordades. Juurdepääsu kontrolli tuleb teha töötlemise ajal kogu andmevoo ulatuses.

56. Lisaks on artikli 25 lõikes 2 sätestatud, et isikuandmeid ei tehta ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks. Vastutav töötleja piirab vaikimisi juurdepääsu ja annab andmesubjektile võimaluse sekkuda enne, kui andmesubjekti isikuandmed avaldatakse või tehakse muul moel määramata füüsiliste isikute ringile kättesaadavaks.

57. Isikuandmete kättesaadavaks tegemine määramata arvule isikutele võib kaasa tuua andmete veelgi ulatuslikuma levitamise, kui algselt kavandatud. See kehtib eriti interneti ja otsingumootorite puhul. See tähendab, et vastutavad töötlejad peaksid vaikimisi andma andmesubjektidele võimaluse sekkuda

[17] Isikuandmete kaitse üldmääruse artikli 4 lõike 2 kohaselt hõlmab see kogumist, dokumenteerimist, korrastamist, struktureerimist, säilitamist, kohandamist ja muutmist, päringute tegemist, lugemist, kasutamist, edastamist, levitamist või muul moel kättesaadavaks tegemist, ühitamist või ühendamist, piiramist, kustutamist või hävitamist.

[18] Artikli 29 töörühma arvamus 05/2014 anonüümimistehnikate kohta. WP 216, 10. aprill 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf.

[19] Vt isikuandmete kaitse üldmääruse artikli 4 lõige 1 ja põhjendus 26 ning artikli 29 töörühma arvamus 05/2014 anonüümimistehnikate kohta. Vt ka käesoleva dokumendi jaotise 3 alajaotist „Säilitamise piirang“, kus on öeldud, et vastutav töötleja peab tagama rakendatava(t)e anonüümimismeetodi(te) tõhususe.

enne isikuandmete kättesaadavaks tegemist avatud internetis. See on eriti oluline laste ja haavatavate rühmade puhul.

58. Sõltuvalt töötlemise õiguslikust alusest võib sekkumisvõimalus olla eri töötlemistoimingute puhul erinev. Näiteks võib küsida andmesubjekti nõusolekut isikuandmete avalikustamiseks või kasutada privaatsusseadeid, et andmesubjektid saaksid ise reguleerida üldsuse juurdepääsu.

59. Isegi kui isikuandmed tehakse avalikult kättesaadavaks andmesubjekti nõusolekul ja tema mõistmisel, ei tähenda see, et mis tahes muu vastutav töötleja, kellel on juurdepääs isikuandmetele, tohib vabalt neid oma eesmärgi täitmiseks töödelda – neil peab olema eraldi õiguslik alus[20].

3 ANDMEKAITSEPÕHIMÕTETE RAKENDAMINE ISIKUANDMETE TÖÖTLEMISEL, KASUTADES LÕIMITUD ANDMEKAITSET JA VAIKIMISI ANDMEKAITSET

60. Vastutav töötleja peab kõikides töötlemistoimingute kavandamise etappides, sh hanked, allhanked, arendamine, tugi, hooldus, katsetamine, säilitamine, kustutamine jne, võtma arvesse ja kaaluma lõimitud andmekaitse ja vaikimisi andmekaitse eri aspekte, mida selgitatakse käesolevas peatükis näidetega, mis on asetatud põhimõtete rakendamise konteksti[21] [22] [23].

61. Vastutavad töötlejad peavad lõimitud ja vaikimisi andmekaitse tagamiseks rakendama andmekaitsepõhimõtteid. Need põhimõtted on läbipaistvus, seaduslikkus, õiglus, eesmärgi piirang, võimalikult väheste andmete kogumine, õigsus, säilitamise piirang, terviklus ja konfidentsiaalsus ning vastutus. Need põhimõtted on esitatud isikuandmete kaitse üldmääruse artiklis 5 ja põhjenduses 39. Et täielikult aru saada sellest, kuidas lõimitud ja vaikimisi andmekaitset rakendada, on oluline mõista iga põhimõtte tähendust.

62. Lõimitud andmekaitse ja vaikimisi andmekaitse rakendamise kohta näidete toomiseks oleme koostanud loetelu iga põhimõtte **peamistest lõimitud andmekaitse ja vaikimisi andmekaitse aspektidest**. Need näited illustreerivad kõnealust konkreetset andmekaitsepõhimõtet, kuid võivad kattuda ka muude tihedalt seotud põhimõtetega. Euroopa Andmekaitsenõukogu rõhutab, et allpool esitatud põhiaspektid ja näited ei ole ammendavad ega siduvad, vaid on mõeldud suunistena iga põhimõtte mõistmiseks. Vastutavad töötlejad peavad hindama, kuidas tagada põhimõtete järgimine kõnealuse konkreetse töötlemistoimingu puhul.

63. Kuigi käesolevas jaotises keskendutakse põhimõtete rakendamisele, peaks vastutav töötleja rakendama ka *asjakohaseid* ja *tõhusaid* meetmeid andmesubjektide õiguste kaitsmiseks, sealhulgas kooskõlas isikuandmete kaitse üldmääruse III peatükiga, kui põhimõtted seda juba ei nõua.

64. Vastutuse põhimõte on üldine: selle kohaselt on vastutava töötleja kohus valida vajalikud tehnilised ja korralduslikud meetmed.

---

[20] Vt kohtuasi nr 931/13, Satakunnan Markkinapörssi Oy ja Satamedia Oy *vs*. Soome.

[21] Veel näiteid on avaldanud Norra andmekaitseasutus: „Software Development with Data Protection by Design and by Default“ (Lõimitud ja vaikimisi andmekaitsega tarkvaraarendus). 28. november 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.

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

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

3.1 Läbipaistvus[24]

65. Vastutav töötleja peab andmesubjekti selgelt ja ausalt teavitama, kuidas isikuandmeid kogutakse, kasutatakse ja jagatakse. Läbipaistvus seisneb selles, et andmesubjektil võimaldatakse mõista ja vajaduse korral kasutada artiklitega 15–22 ette nähtud õigusi. Põhimõte on lõimitud artiklitesse 12, 13, 14 ja 34. Läbipaistvuse põhimõtte toetamiseks kehtestatud meetmed ja kaitsemeetmed peavad toetama ka nende artiklite rakendamist.

66. Läbipaistvuse põhimõtte lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:

- selgus – teave peab olema koostatud selges ja lihtsas keeles ning olema sisutihe ja arusaadav;
- semantika – edastataval teabel peab olema kõnealusele sihtrühmale selge tähendus;
- juurdepääsetavus – teave peab olema andmesubjektile hõlpsasti ligipääsetav;
- kontekstipõhine – teave tuleb esitada asjakohasel ajal ja sobivas vormis;
- asjakohasus – teave peab olema asjakohane ja konkreetsele andmesubjektile kohaldatav;
- universaalsus – teave peab olema ligipääsetav kõigile ning hõlmama masinloetavate keelte kasutamise võimalust, et hõlbustada ja automatiseerida loetavust ning soodustada selgust;
- mõistetavus – andmesubjektidel peab olema selge arusaam sellest, mida nad võivad eeldada seoses oma isikuandmete töötlemisega, eelkõige juhul, kui andmesubjektideks on lapsed või muud haavatavad rühmad;
- mitmekanalilisus – lisaks teabe esitamisele teksti kujul tuleb teavet anda eri kanalites ja meediumites, et teave jõuaks suurema tõenäosusega tõhusalt andmesubjektini;
- kihilisus – teave tuleks esitada kihiliselt, et tagada tasakaal tervikluse ja mõistmise vahel, võttes samal ajal arvesse andmesubjektide mõistlikke ootusi.

Näide[25]

Läbipaistvuse nõuete täitmiseks töötab vastutav töötleja välja privaatsuspõhimõtted, et avaldada need oma veebisaidil. Need ei tohiks sisaldada liiga palju teavet, kuna sellist pikka teksti on keskmisel andmesubjektil raske läbi töötada ja mõista. Need põhimõtted peavad olema kirjutatud selges ja arusaadavas keeles, et veebisaidi kasutajal oleks lihtne mõista, kuidas tema isikuandmeid töödeldakse. Seepärast annab vastutav töötleja teavet kihiliselt, tõstes esile kõige olulisemad punktid. Üksikasjalikum teave on kergesti kättesaadav. Privaatsuspõhimõtete eri osade ja mõistete lähemaks selgitamiseks kasutatakse rippmenüüsid ja linke teistele lehtedele. Ühtlasi tagab vastutav töötleja, et teavet antakse mitme kanali kaudu, pakkudes kirjaliku teabe kõige olulisemate punktide selgitamiseks videoklippe. Eri leheküljed peavad kindlasti olema üksteisega kooskõlas, et kihilisus ei suurendaks segadust, vaid pigem vähendaks seda.

Privaatsuspõhimõtted ei tohi olla andmesubjektidele raskesti ligipääsetavad. Seetõttu tehakse need kättesaadavaks ja nähtavaks kõikidel kõnealuse veebisaidi lehekülgedel, et andmesubjekt pääseks privaatsusteabele ligi vaid ühe hiireklõpsuga. Esitatav teave on ühtlasi koostatud kooskõlas universaalsuse parimate tavade ja standarditega, et see oleks kõigile ligipääsetav.

Lisaks tuleb vajalik teave esitada õigel ajal ja õiges kontekstis. Kuna vastutav töötleja teeb veebisaidil kogutud andmetega mitmeid töötlemistoiminguid, ei piisa läbipaistvuse nõuete täitmiseks üksnes

[24] Läbipaistvuse mõistet on täpsemalt selgitatud artikli 29 töörühma suunistes määruse 2016/679 kohase läbipaistvuse kohta. WP 260 rev.01, 11. aprill 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 – kinnitanud Euroopa Andmekaitsenõukogu.

[25] Prantsusmaa andmekaitseasutus on avaldanud mitu näidet kasutajate teavitamise parimate tavade ja muude läbipaistvuspõhimõtete kohta: https://design.cnil.fr/en/.

veebisaidil esitatavatest üldistest privaatsuspõhimõtetest. Seetõttu loob vastutav töötleja teabevoo, esitades andmesubjektile asjakohase teabe asjakohases kontekstis, kasutades näiteks teabekilde või hüpikaknaid. Näiteks kui vastutav töötleja palub andmesubjektil isikuandmeid esitada, teavitab ta andmesubjekti sellest, kuidas isikuandmeid töödeldakse ja miks need isikuandmed on töötlemiseks vajalikud.

3.2 Seaduslikkus

67. Vastutav töötleja peab määrama isikuandmete töötlemiseks kehtiva õigusliku aluse. Meetmed ja kaitsemeetmed peaksid aitama täita nõuet tagada, et kogu töötlemisprotsess vastaks töötlemise asjakohasele õiguslikule alusele.

68. Seaduslikkuse põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - asjakohasus – töötlemisele tuleb kohaldada õiget õiguslikku alust;
    - eristamine[26] – eristatakse iga töötlemistoimingu puhul kasutatavat õiguslikku alust;
    - eriotstarve – asjakohane õiguslik alus peab olema selgelt seotud töötlemise konkreetse eesmärgiga[27];
    - vajalikkus – et töötlemine oleks seaduslik, peab see olema eesmärgi saavutamiseks vältimatult vajalik;
    - autonoomia – andmesubjektidele tuleb anda oma isikuandmete üle kontrolli omamisel õigusliku aluse piires võimalikult suur autonoomia;
    - nõusoleku saamine – nõusolek peab olema vabatahtlikult antud, konkreetne, teadlik ja üheselt mõistetav[28]. Erilist tähelepanu tuleks pöörata laste ja noorte suutlikkusele anda teadlik nõusolek;
    - nõusoleku tagasivõtmine – kui õiguslik alus on nõusolek, peab töötlemine võimaldama nõusoleku hõlpsalt tühistada. Nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine. Vastasel juhul ei ole vastutava töötleja nõusoleku andmise mehhanism kooskõlas isikuandmete kaitse üldmäärusega[29];
    - huvide tasakaalustamine – kui õiguslik alus on õigustatud huvi, peab vastutav töötleja huvisid kaaluma, pöörates erilist tähelepanu võimu ebavõrdsusele, eelkõige alla 18-aastastele lastele ja teistele haavatavatele rühmadele. Andmesubjektidele avalduva negatiivse mõju leevendamiseks nähakse ette meetmed ja kaitsemeetmed;
    - eelnev kindlaksmääramine – õiguslik alus tuleb kindlaks määrata enne töötlemise toimumist;
    - kehtivuse lõppemine – kui õiguslik alus kaotab kehtivuse, peab vastavalt lõppema ka töötlemine;
    - kohandamine – kui on olemas töötlemise õigusliku aluse kehtiv muudatus, tuleb tegelikku töötlemist kohandada vastavalt uuele õiguslikule alusele[30];

[26] Euroopa Andmekaitsenõukogu suunised 2/2019 isikuandmete töötlemise kohta isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti b alusel seoses andmesubjektidele internetipõhiste teenuste osutamisega. Versioon 2.0, 8. oktoober 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_et.pdf.

[27] Vt eesmärgi piirangu jaotist allpool.

[28] Vt suunised 05/2020 määruse 2016/679 kohase nõusoleku kohta. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[29] Vt suunised 05/2020 määruse 2016/679 kohase nõusoleku kohta, lk 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[30] Kui algne õiguslik alus on nõusolek, vt suunised 05/2020 määruse 2016/679 kohase nõusoleku kohta. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

- vastutusvaldkondade jaotamine – kui ette on nähtud kaasvastutus, peavad pooled vastutuse andmesubjekti ees selgel ja läbipaistval viisil ära jagama ning kavandama andmete töötlemise meetmed sellele vastavalt.

Näide

Pank plaanib pakkuda laenurakenduste haldamise tõhusust parandavat teenust. Teenuse idee seisneb selles, et pank saab kliendilt luba küsides hankida kliendi kohta andmeid otse maksuametilt. Selles näites ei käsitleta muudest allikatest pärit isikuandmete töötlemist.

Andmesubjekti finantsolukorra tõendamiseks on vaja isikuandmeid hankida, et andmesubjekti taotluse alusel oleks võimalik võtta laenulepingu sõlmimisele eelnevaid meetmeid[31]. Siiski ei peeta vajalikuks koguda isikuandmeid otse maksuametilt, sest klient saab sõlmida lepingu ka nii, et esitab maksuametilt saadud teabe ise. Kuigi pangal võib olla õigustatud huvi saada dokumendid otse maksuametilt, näiteks selleks, et tagada laenude tõhus menetlemine, kujutab pankade otsene juurdepääs taotlejate isikuandmetele endast ohtu seoses juurdepääsuõiguste kasutamise või võimaliku kuritarvitamisega.

Seaduslikkuse põhimõtte rakendamisel mõistab vastutav töötleja, et kõnealusel juhul ei saa ta selle töötlemise osa puhul, mis hõlmab isikuandmete kogumist otse maksuametilt, kasutada õigusliku alusena vajalikkust lepingu sõlmimiseks. Tõsiasi, et selle konkreetse töötlemisega kaasneb oht, et andmesubjekt on oma andmete töötlusse vähem kaasatud, on töötlemise enda seaduslikkuse hindamisel samuti asjakohane tegur. Pank järeldab, et see töötlemise osa peab põhinema muul õiguslikul alusel. Liikmesriigis, kus vastutav töötleja asub, kehtivad riiklikud õigusaktid, mille kohaselt tohib pank koguda teavet otse maksuametilt, kui andmesubjekt on selleks eelnevalt nõusoleku andnud.

Seetõttu annab pank võrgurakenduse platvormil töötlemise kohta teavet viisil, mis võimaldab andmesubjektidel lihtsalt mõista, milline töötlemine on kohustuslik ja milline on valikuline. Vaikimisi töötlemisvalikud ei luba hankida andmeid muudelt allikatelt kui andmesubjektilt endalt ning teabe otse ametiasutuselt hankimise valik esitatakse viisil, mis ei takista andmesubjekti sellest keeldumast. Nõusolek, mis on antud otse teistelt vastutavatelt töötlejatelt andmete kogumiseks, on ajutine teatud teabele juurdepääsu õigus.

Antud nõusolekut töödeldakse elektrooniliselt ja see dokumenteeritakse ning andmesubjektidel võimaldatakse lihtsalt kontrollida, millele nad on nõusoleku andnud, ja oma nõusolek tagasi võtta.

Vastutav töötleja on neid lõimitud andmekaitse ja vaikimisi andmekaitse nõudeid eelnevalt hinnanud ning lisab kõik need kriteeriumid oma platvormi hanke nõuete kirjeldusse. Vastutav töötleja on teadlik sellest, et kui ta ei lisa lõimitud andmekaitse ja vaikimisi andmekaitse nõudeid hankesse, võib hiljem olla liiga hilja andmekaitse rakendamiseks või see võib olla väga kulukas protsess.

3.3 Õiglus

69. Õiglus on üldine põhimõte, mille kohaselt ei tohi isikuandmeid töödelda andmesubjekti põhjendamatult kahjustaval, ebaseaduslikult diskrimineerival, eksitaval või talle ettearvamatul viisil. Meetmed ja kaitsemeetmed, millega rakendatakse õigluse põhimõtet, toetavad ka andmesubjektide õigusi ja vabadusi, eelkõige õigust saada teavet (läbipaistvus), sekkumise õigust (juurdepääs,

[31] Vt isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt b.

kustutamine, andmete ülekantavus, parandamine) ning töötlemise piiramise õigust (andmesubjektide õigus sellele, et nende kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel, ning andmesubjektide õigus sellele, et neid ei diskrimineeritaks).

70. Õigluse põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
- sõltumatus – andmesubjektidele tuleks anda võimalikult suur autonoomia otsustamisel, kuidas nende isikuandmeid kasutatakse ning millised on sellise kasutamise või töötlemise ulatus ja tingimused;
- suhtlus – andmesubjektidel peab olema võimalik pöörduda vastutava töötleja poole ja kasutada oma õigusi seoses töödeldavate isikuandmetega;
- ootused – töötlemine peab vastama andmesubjektide mõistlikele ootustele;
- mittediskrimineerimine – vastutav töötleja ei tohi andmesubjektide vahel ebaõiglaselt vahet teha;
- ärakasutamisest hoidumine – vastutav töötleja ei tohi ära kasutada andmesubjektide vajadusi ega kaitsetust;
- tarbijate valik – vastutav töötleja ei tohi kasutajaid ebaõiglaselt endaga siduda. Kui isikuandmeid töötlev teenus on ärisaladusega kaitstud, võib sellega kaasneda teenusest sõltumine, mis ei pruugi olla õiglane, kui see kahjustab andmesubjektide võimalust kasutada oma andmete ülekandmise õigust kooskõlas artikliga 20;
- võimutasakaal – võimutasakaal peaks olema vastutava töötleja ja andmesubjekti suhte peamine eesmärk. Võimu ebavõrdsust tuleks vältida. Kui see ei ole võimalik, tuleks võimu ebavõrdsust arvesse võtta ja rakendada sobivaid vastumeetmeid;
- riski ülekandmisest hoidumine – vastutavad töötlejad ei tohi kanda ettevõtte riske üle andmesubjektidele;
- pettuse vältimine – andmetöötlusteave ja -valikud tuleks esitada objektiivsel ja neutraalsel viisil, vältides mis tahes eksitavat või manipuleerivat keelekasutust või kujundust;
- õiguste austamine – vastutav töötleja peab austama andmesubjektide põhiõigusi ning rakendama asjakohaseid meetmeid ja kaitsemeetmeid ning ei tohi neid õigusi piirata, välja arvatud juhul, kui see on seadusega sõnaselgelt põhjendatud;
- eetiline – vastutav töötleja peab nägema töötlemise laiemat mõju üksikisiku õigustele ja väärikusele;
- tõene – vastutav töötleja peab tegema kättesaadavaks teabe selle kohta, kuidas ta isikuandmeid töötleb, tegutsema nii, nagu lubab, ega tohi andmesubjekte eksitada;
- inimsekkumine – vastutav töötleja peab kaasama *kvalifitseeritud* inimsekkumise, millega suudetakse tuvastada masinate genereeritud võimalik kallutatus, et kaitsta andmesubjektile artikliga 22 ette nähtud õigust, et tema kohta ei tehtaks üksnes automatiseeritud töötlusel põhinevaid otsuseid[32];
- õiglased algoritmid – hinnata korrapäraselt, kas algoritmid toimivad kooskõlas eesmärkidega, ning kohandada algoritme, et leevendada tuvastatud kallutatust ja tagada õiglane töötlemine. Andmesubjekte tuleb teavitada sellest, et isikuandmeid töödeldakse algoritmide põhjal, mis analüüsivad või prognoosivad näiteks andmeid, mis on seotud töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, usaldusväärsuse või käitumise, asukoha või liikumisega[33].

[32] Vt suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta määruse 2016/679 kohaldamisel, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
[33] Vt isikuandmete kaitse üldmääruse põhjendus 71.

Näide 1

Vastutav töötleja käitab otsingumootorit, mis töötleb peamiselt kasutaja loodud isikuandmeid. Vastutavale töötlejale on kasulik, kui tal on suur hulk isikuandmeid ja tal on võimalik neid kasutada suunatud reklaamide jaoks. Seetõttu soovib vastutav töötleja andmesubjekte mõjutada, et nad lubaksid oma isikuandmeid laialdasemalt koguda ja kasutada. Nõusoleku saamiseks esitatakse andmesubjektile töötlemisvalikud.

Õigluse põhimõtte rakendamisel, võttes arvesse töötlemise laadi, ulatust, konteksti ja eesmärki, mõistab vastutav töötleja, et ta ei saa esitada valikuid viisil, mis mõjutaks andmesubjekti andma vastutavale töötlejale luba koguda rohkem isikuandmeid, kui seda võimaldaks olukord, kus valikud on esitatud ühesugusel ja neutraalsel viisil. See tähendab, et ta ei saa esitada töötlemise valikuid viisil, mis raskendab andmesubjektidel oma andmete jagamisest keeldumist või privaatsusseadete muutmist ja töötlemise piiramist. Sel viisil toimimine oleks vastuolus artikli 25 põhimõtetega. Töötlemise vaikevalikud ei tohiks olla sekkuvad ning edasise töötlemise valik tuleb esitada viisil, mis ei survesta andmesubjekti nõusolekut andma. Seetõttu esitab vastutav töötleja nõusoleku andmise või sellest loobumise võimalused kui kaks võrdselt nähtavat valikut, selgitades iga valiku mõju andmesubjektile.

Näide 2

Teine vastutav töötleja töötleb isikuandmeid voogedastuse teenuse osutamiseks, mille puhul kasutajad saavad valida standardkvaliteediga tavatellimuse ja kvaliteetsema preemiumtellimuse vahel. Osana preemiumtellimusest pakutakse tellijatele eelisjärjekorras klienditeenindust.

Õigluse põhimõtte kohaselt ei tohi preemiumtellijatele eelisjärjekorras pakutav klienditeenindus diskrimineerida tavatellijaid, takistades neil kasutada oma õigusi kooskõlas isikuandmete kaitse üldmääruse artikliga 12. See tähendab, et kuigi preemiumtellijad saavad teenust eelisjärjekorras, ei tohi see põhjustada olukorda, kus puuduvad asjakohased meetmed tavatellijate taotlustele vastamiseks põhjendamata viivituseta ja igal juhul ühe kuu jooksul alates taotluse laekumisest.

Prioriteetseteks peetavad kliendid võivad maksta, et saada paremat teenust, kuid kõigil andmesubjektidel peab olema võrdne võimalus kasutada oma õigusi ja vabadusi, nagu on ette nähtud artikliga 12.

3.4 Eesmärgi piirang[34]

71. Vastutav töötleja peab andmeid koguma täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning ei tohi andmeid hiljem töödelda viisil, mis on vastuolus eesmärkidega, milleks neid koguti[35]. Töötlemine tuleks seega kavandada selle alusel, mis on eesmärkide saavutamiseks vajalik. Kui toimub muu edasine töötlemine, peab vastutav töötleja kõigepealt veenduma, et töötlemise

[34] Artikli 29 töörühm esitas suunised direktiivi 95/46/EÜ kohase eesmärgi piirangu põhimõtte mõistmiseks. Kuigi Euroopa Andmekaitsenõukogu ei ole arvamust vastu võtnud, võib see olla siiski asjakohane, kuna põhimõtte sõnastus on isikuandmete kaitse üldmääruse kohaselt sama. Artikli 29 töörühma arvamus 03/2013 eesmärgi piirangu kohta. WP 203, 2. aprill 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt b.

eesmärgid on kooskõlas algsete eesmärkidega, ja kavandama töötlemise vastavalt sellele. Seda, kas uus eesmärk on kooskõlas või mitte, tuleb hinnata artikli 6 lõikes 4 esitatud kriteeriumide alusel.

72. Eesmärgi piirangu põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - ettemääratus – õiguspärased eesmärgid tuleb kindlaks määrata enne töötlemise kavandamist;
    - spetsiifilisus – eesmärgid tuleb täpselt määratleda, et oleks selge, miks isikuandmeid töödeldakse;
    - eesmärgikohasus – töötlemine tuleb kavandada ja töötlemise piirid kehtestada lähtuvalt töötlemise eesmärgist;
    - vajalikkus – eesmärk määrab, milliseid isikuandmeid on töötlemiseks vaja;
    - vastavus – iga uus eesmärk peab olema kooskõlas andmete kogumise algse eesmärgiga ning selle põhjal tuleb teha meetodis asjakohaseid muudatusi;
    - edasise töötlemise piiramine – vastutav töötleja ei tohi ühendada andmekogumeid ega teostada edasist töötlust uute eesmärkide täitmiseks, mis pole algsetega kooskõlas;
    - taaskasutamise piirangud – vastutav töötleja peab kasutama tehnilisi meetmeid, sh räsimist ja krüpteerimist, et piirata isikuandmete uuteks eesmärkideks kasutamise võimalust. Vastutaval töötlejal peaksid olema ka korralduslikud meetmed, nagu põhimõtted ja lepingulised kohustused, mis piiravad isikuandmete taaskasutamist;
    - kontrollimine – vastutav töötleja peab korrapäraselt kontrollima, kas töötlemine on vajalik nende eesmärkide täitmiseks, milleks andmed koguti, ning kas meetod on kooskõlas eesmärgi piiranguga.

Näide

Vastutav töötleja töötleb oma klientide isikuandmeid. Töötlemise eesmärk on lepingu täitmine, s.o et oleks võimalik tarnida kaupu õigel aadressil ja saada tasu. Säilitatavad isikuandmed on ostutehingute ajalugu, nimi, aadress, e-posti aadress ja telefoninumber.

Vastutav töötleja kaalub kliendisuhete haldamise toote ostmist, mis koondaks ühte kohta kokku kõik klientide andmed seoses müügi, turustamise ja klienditeenindusega. Toode võimaldab säilitada kõiki telefonikõnesid, tegevusi, dokumente, e-kirju ja turunduskampaaniad, et saada kliendist täielik ülevaade. Lisaks saab kliendisuhete haldamise toode automaatselt analüüsida klientide ostujõudu, kasutades selleks avalikku teavet. Analüüsi eesmärk on reklaamitegevust paremini suunata. Töötlemise algne õiguspärane eesmärk neid tegevusi ei hõlma.

Eesmärgi piirangu põhimõtte järgimiseks palub vastutav töötleja toote tarnijal kaardistada eri töötlemistoimingud, milles kasutatakse isikuandmeid vastutava töötleja jaoks asjakohastel eesmärkidel.

Pärast kaardistamistulemuste saamist hindab vastutav töötleja, kas uus turunduseesmärk ja suunatud reklaami eesmärk on kooskõlas andmete kogumisel määratletud algsete eesmärkidega ning kas vastavaks töötlemiseks on olemas piisav õiguslik alus. Kui hindamisel leitakse, et see pole nii, ei kasuta vastutav töötleja neid funktsioone. Teise võimalusena võib vastutav töötleja loobuda hindamisest ja lihtsalt mitte kasutada toote neid funktsioone.

3.5 Võimalikult väheste andmete kogumine

73. Töödelda võib vaid isikuandmeid, mis on piisavad, asjakohased ja piirduvad sellega, mis on eesmärgi täitmise seisukohast **vajalik**[36]. Seepärast peab vastutav töötleja eelnevalt kindlaks määrama, millised töötlemissüsteemide funktsioonid ja parameetrid on lubatud. Võimalikult väheste andmete kogumine aitab järgida ja rakendada vajalikkuse põhimõtet. Edasisel töötlemisel peab vastutav töötleja korrapäraselt kaaluma, kas töödeldavad isikuandmed on endiselt piisavad, asjakohased ja vajalikud või kas andmed tuleks kustutada või anonüümseks muuta.

74. Vastutavad töötlejad peavad kõigepealt kindlaks määrama, kas neil on oma asjakohaste eesmärkide saavutamiseks üldse vaja isikuandmeid töödelda. Vastutav töötleja peaks kontrollima, kas asjaomaseid eesmärke on võimalik saavutada, töödeldes vähem isikuandmeid või omades vähem üksikasjalikke või kokkuvõtlikke isikuandmeid või ilma et peaks üldse isikuandmeid töötlema[37]. Selline kontroll peaks toimuma enne mis tahes töötlemist, kuid seda võiks teha ka töötlemisprotsessi mis tahes etapis. See on kooskõlas ka artikliga 11.

75. Võimalikult väheste andmete kogumine võib viidata ka tuvastamise ulatusele. Kui töötlemise eesmärgi puhul ei pea lõplik andmekogum viitama tuvastatud või tuvastatavale isikule (nagu statistika puhul), kuid algse töötlemise puhul peab (nt enne andmete koondamist), siis tuleb vastutaval töötlejal isikuandmed kustutada või anonüümseks muuta niipea, kui tuvastamine ei ole enam vajalik. Kui edasine tuvastamine on teiste töötlemistoimingute puhul siiski vajalik, tuleb andmesubjektide õigustega seotud ohtude vähendamiseks andmed pseudonüümida.

76. Võimalikult väheste andmete kogumise põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - andmetest hoidumine – hoiduda isikuandmete töötlemisest üldse, kui see on asjaomase eesmärgi puhul võimalik;
    - piirang – piirata kogutavate isikuandmete hulka üksnes eesmärgi saavutamiseks vajaliku hulgani;
    - juurdepääsupiirang – kavandada andmete töötlemine nii, et oma ülesannete täitmiseks vajab isikuandmetele juurdepääsu minimaalne arv inimesi, ning vastavalt piirata juurdepääsu;
    - asjakohasus – isikuandmed peavad olema kõnealuse töötlemise seisukohalt asjakohased ning vastutav töötleja peab suutma asjakohasust tõendada;
    - vajalikkus – iga isikuandmete liik peab olema täpselt kindlaksmääratud eesmärkide saavutamiseks vajalik ning neid tuleks töödelda vaid juhul, kui eesmärki ei ole võimalik muude vahenditega saavutada;
    - koondamine – võimaluse korral kasutada koondatud andmeid;
    - pseudonüümimine – pseudonüümida isikuandmed niipea, kui otse tuvastavaid isikuandmeid ei ole enam vaja, ning säilitada identifitseerimisvõtmeid eraldi;
    - anonüümseks muutmine ja kustutamine – kui isikuandmed ei ole või ei ole enam eesmärgi saavutamiseks vajalikud, tuleb isikuandmed anonüümseks muuta või kustutada;
    - andmevoog – andmevoog tuleb teha piisavalt tõhusaks, et ei loodaks vajalikust rohkem koopiaid;
    - teaduse ja tehnoloogia viimane areng – vastutav töötleja peab kasutama nüüdisaegseid ja sobivaid andmetest hoidumise ja võimalikult väheste andmete kogumise tehnoloogiaid.

[36] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

[37] Isikuandmete kaitse üldmääruse põhjenduses 39 on sätestatud: „Isikuandmeid tuleks töödelda vaid juhul, kui nende töötlemise eesmärki ei ole mõistlikult võimalik saavutada muude vahendite abil“.

Näide 1

Raamatupood soovib suurendada oma tulu raamatute veebis müümisega. Raamatupoe omanik soovib koostada standarditud tellimisvormi. Et kliendid täidaksid kõik talle vajaliku teabe väljad, muudab raamatupoe omanik kõik vormi väljad kohustuslikeks (kui klient ei täida kõiki välju, ei saa ta tellimust esitada). Veebipoe omanik kasutab algselt standardset kontaktandmete vormi, kus küsitakse kliendi sünniaega, telefoninumbrit ja kodust aadressi. Siiski ei ole kõik vormi väljad raamatute ostu ja tarne eesmärgi täitmiseks vajalikud. Kui andmesubjekt maksab toote eest ette, ei ole andmesubjekti sünniaeg ja telefoninumber sel konkreetsel juhul toote ostmiseks vajalikud. See tähendab, et need väljad ei saa olla veebivormil toote tellimiseks kohustuslikud, välja arvatud juhul, kui vastutav töötleja suudab selgelt tõendada, et seda teavet on vaja muuks otstarbeks ja miks on väljad vajalikud. Lisaks on olukordi, kus aadressi ei ole vaja. Näiteks e-raamatu tellimisel saab klient toote alla laadida otse oma seadmesse.

Veebipoe omanik otsustab seetõttu koostada kaks veebivormi: kliendi aadressi väljaga veebivormi raamatute tellimiseks ja ilma kliendi aadressi väljata veebivormi e-raamatute tellimiseks.

Näide 2

Ühistranspordiettevõte soovib koguda reisijate marsruutidel põhinevat statistilist teavet. See aitab teha ühistranspordigraafikute muutmisel õigeid valikuid ning panna paika õigeid rongiliine. Reisijad peavad pileti lugejas registreerima iga kord, kui nad sisenevad transpordivahendisse või väljuvad sellest. Vastutav töötleja hindab reisijate reisimarsruutide kogumisega seotud riske reisijate õigustele ja vabadustele ning teeb kindlaks, et reisijaid on võimalik piletituvastiga marsruudi järgi tuvastada, kui nad elavad või töötavad hõredalt asustatud piirkondades. Kuna see ei ole ühistranspordigraafikute ja rongiliinide optimeerimiseks vajalik, ei säilita vastutav töötleja piletituvasti andmeid. Kui reis on lõppenud, säilitab vastutav töötleja vaid eraldi reisimarsruudid, nii et üksiku piletiga seotud reise ei ole võimalik tuvastada ja alles jääb vaid teave eraldi reisimarsruutide kohta.

Juhtudel, kui säilib ühistranspordi reisimarsruudi järgi isiku tuvastamise oht, rakendab vastutav töötleja statistilisi meetmeid, näiteks lõigates ära reisi alguse ja lõpu.

Näide 3

Kuller soovib hinnata oma tarnete tõhusust tarneaja, töökoormuse kavandamise ja kütusekulu põhjal. Selleks peab kuller töötlema palju nii töötajate (juhid) kui ka klientide isikuandmeid (aadressid, tarnitav kaup jne). Selle töötlemistoiminguga kaasneb nii töötajate jälgimise oht, mille puhul on vaja spetsiaalseid õiguslikke kaitsemeetmeid, kui ka klientide harjumuste jälgimise oht, kuna aja jooksul tarnitud kaubad on teada. Neid riske saab märkimisväärselt vähendada töötajate ja klientide nõuetekohase pseudonüümimisega. Kui pseudonüümimise võtmeid vahetatakse sageli ja üksikasjalike aadresside asemel võetakse arvesse makropiirkondi, tagatakse tõhusalt võimalikult väheste andmete kogumine ning vastutav töötleja saab keskenduda üksnes tarneprotsessile ja ressursside optimeerimise eesmärgile, ilma et tegemist oleks üksikisikute (klientide või töötajate) käitumise jälgimisega.

Näide 4

Haigla kogub andmeid oma patsientide kohta haigla infosüsteemis (elektrooniline tervisekaart). Haiglatöötajad peavad patsientide toimikutele juurde pääsema, et saada teavet patsientide hoolduse ja ravi üle otsustamiseks, ning dokumenteerima kõik diagnostika-, hooldus- ja ravitoimingud. Vaikimisi antakse juurdepääs ainult nendele meditsiinitöötajatele, kes on määratud tegelema vastava patsiendiga osakonnas, kus ta töötab. Patsiendi toimikule juurdepääsu omavate inimeste arvu suurendatakse, kui raviga on seotud teised osakonnad või diagnostikaüksused. Pärast patsiendi haiglast lahkumist ja arvete esitamist võimaldatakse juurdepääs vaid väikesele arvule töötajatele igast osakonnast, kes vastavad patsiendi loal teiste meditsiiniteenuste osutajate esitatud meditsiinilise teabe päringutele või konsultatsioonidele.

3.6 Õigsus

77. Isikuandmed on õiged ja ajakohastatud ning võetakse kõik mõistlikud meetmed, et viivitamata kustutada või parandada andmete töötlemise eesmärgi seisukohast ebaõiged isikuandmed[38].

78. Nõudeid tuleb käsitleda andmete konkreetse kasutusotstarbe ohtude ja tagajärgede kontekstis. Ebaõiged isikuandmed võivad ohustada andmesubjektide õigusi ja vabadusi, näiteks kui nende tõttu pannakse vale diagnoos või käsitletakse valesti tervishoiuprotokolli või kui ebaõige pilt isikust võib viia otsusteni, mis langetatakse valedel alustel kas manuaalselt, automatiseeritud otsuste langetamist kasutades või tehisintellekti abil.

79. Õigsuse põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - andmeallikas – isikuandmete allikad peavad olema andmete õigsuse seisukohast usaldusväärsed;
    - õigsuse määr – iga isikuandmete element peab olema nii õige, kui see on määratud eesmärkide saavutamiseks vajalik;
    - mõõdetav õigsus – vähendada valepositiivsete/negatiivsete tulemuste arvu, näiteks kallutatust automatiseeritud otsustes ja tehisintellektis;
    - kontrollimine – olenevalt andmete laadist, eelkõige sellest, kui sageli need võivad muutuda, peab vastutav töötleja kontrollima andmesubjekti isikuandmete õigsust enne töötlemist ja töötlemise eri etappide ajal (nt vanusepiirangud);
    - kustutamine/parandamine – vastutav töötleja peab ebaõiged andmed viivitamata kustutama või parandama. Vastutav töötleja peab seda hõlpsasti võimaldama eelkõige juhul, kui andmesubjektid on või olid lapsed ja soovivad hiljem sellised isikuandmed eemaldada[39];
    - vigade kuhjumise vältimine – vastutavad töötlejad peavad vähendama töötlemisahelas kuhjunud vigade mõju;
    - juurdepääs – andmesubjektidele tuleb kooskõlas isikuandmete kaitse üldmääruse artiklitega 12–15 anda teavet isikuandmete kohta ja lihtne juurdepääs isikuandmetele, et kontrollida andmete õigsust ja vajaduse korral teha parandusi;
    - pidev õigsus – isikuandmed peavad olema kõigis töötlemise etappides õiged ning kriitilistes järkudes tuleb õigsust kontrollida;
    - ajakohasus – isikuandmeid tuleb ajakohastada, kui see on eesmärgi saavutamiseks vajalik;

[38] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt d.
[39] Vt põhjendus 65.

- andmete esitamise viis – ebatäpsuse vähendamiseks kasutatakse andmete esitamisel tehnoloogilisi ja korralduslikke meetodeid, näiteks vaba teksti väljade asemel esitatakse kokkuvõtlikud eelnevalt kindlaksmääratud valikud.

Näide 1

Kindlustusandja soovib kasutada tehisintellekti, et koostada kindlustust ostvate klientide profiilid, mille põhjal ta teeb kindlustusriski arvutamisel otsuseid. Otsustades, kuidas tehisintellekti lahendused tuleks välja töötada, määrab ettevõte kindlaks töötlemisvahendid ja peab võtma arvesse lõimitud andmekaitset, kui ta valib müüja pakutava hulgast tehisintellekti ja teeb otsuseid tehisintellekti õpetamise kohta.

Tehisintellekti õpetamise viisi kindlaksmääramisel peavad vastutaval töötlejal olema täpsete tulemuste saavutamiseks õiged andmed. Seetõttu peab vastutav töötleja tagama, et tehisintellekti õpetamiseks kasutavad andmed on õiged.

Võttes arvesse, et tal on kehtiv õiguslik alus kasutada tehisintellekti õpetamiseks suurest olemasolevate klientide andmekogust pärinevaid isikuandmeid, valib vastutav töötleja ka moonutuste vältimiseks välja elanikkonda esindava kliendibaasi.

Seejärel kogutakse kliendiandmed vastavast andmekäitlussüsteemist, sealhulgas andmed kindlustuse liigi kohta, näiteks tervisekindlustus, kodukindlustus, reisikindlustus jne, ning andmed avalikest registritest, millele ettevõttel on seaduslik juurdepääs. Kõik andmed pseudonüümitakse enne nende edastamist tehisintellektimudeli õpetamiseks kasutatavasse süsteemi.

Selleks et tehisintellekti õpetamiseks kasutatavad andmed oleksid võimalikult õiged, kogub vastutav töötleja andmeid vaid korrektse ja ajakohastatud teabega andmeallikatest.

Kindlustusandja kontrollib, kas tehisintellekt on usaldusväärne ja annab mittediskrimineerivaid tulemusi nii selle väljatöötamise ajal kui ka hiljem enne toote turulelaskmist. Kui tehisintellekt on täielikult välja õpetatud ja toimib, kasutab kindlustusandja tulemusi kindlustusriskide hindamisel, kuid ei toetu kindlustuse andmise üle otsustamisel üksnes tehisintellektile, välja arvatud juhul, kui otsus tehakse kooskõlas isikuandmete kaitse üldmääruse artikli 22 lõikes 2 sätestatud eranditega.

Kindlustusandja vaatab ka tehisintellekti tulemused korrapäraselt läbi, et säilitada usaldusväärsus ja vajaduse korral algoritmi kohandada.

Näide 2

Vastutav töötleja on tervishoiuasutus, mis püüab leida meetodeid oma kliendiregistrites sisalduvate isikuandmete terviklikkuse ja õigsuse tagamiseks.

Olukordades, kus samal ajal saabub asutusse kaks isikut, kes saavad sama ravi, on oht nad omavahel segamini ajada, kui ainus nende eristamise parameeter on nimi. Õigsuse tagamiseks on vastutaval töötlejal vaja iga isiku jaoks kordumatut identifikaatorit ning seega rohkem teavet kui lihtsalt kliendi nime.

Asutus kasutab mitut klientide isikuandmeid sisaldavat süsteemi ning peab tagama kogu aeg kõikides süsteemides kliendiga seotud teabe korrektsuse, õigsuse ja järjepidevuse. Asutus on tuvastanud mitmed ohud, mis võivad tekkida, kui ühes süsteemis muudetakse teave ära, aga teistes mitte.

Vastutav töötleja otsustab riski vähendada räsimise tehnika abil, mida saab kasutada ravipäeviku andmete terviklikkuse tagamiseks. Ravipäevikute registri ja sellega seotud töötaja jaoks luuakse muudetamatud krüptograafilised ajatemplid, nii et mis tahes muudatus on vajaduse korral ära tuntav, seostatav ja kindlaks tehtav.

3.7 Säilitamise piirang

80. Vastutav töötleja peab tagama, et isikuandmeid hoitaks vormingus, mis võimaldab andmesubjekte identifitseerida vaid seni, kuni see on vajalik nende eesmärkide saavutamiseks, milleks isikuandmeid töödeldakse[40].
On väga oluline, et vastutav töötleja teaks täpselt, milliseid isikuandmeid ettevõte töötleb ja miks. Töötlemise eesmärk on põhikriteerium, mille alusel otsustatakse, kui kaua isikuandmeid säilitatakse.

81. Meetmed ja kaitsemeetmed, millega rakendatakse säilitamise piirangu põhimõtet, täiendavad andmesubjektide õigusi ja vabadusi, täpsemalt õigust andmete kustutamisele ja õigust esitada vastuväiteid.

82. Säilitamise piirangu põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - kustutamine ja anonüümimine – vastutaval töötlejal peaksid olema selged asutusesisesed menetlused ja funktsioonid andmete kustutamiseks ja/või anonüümimiseks;
    - anonüümimise/kustutamise tõhusus – vastutav töötleja tagab, et anonüümitud andmeid ei ole võimalik uuesti identifitseerida ega kustutatud andmeid taastada, ning ta peaks katsetama, kas seda on võimalik teha;
    - automatiseerimine – teatud isikuandmete kustutamine peaks olema automatiseeritud;
    - säilitamiskriteeriumid – vastutav töötleja peab kindlaks määrama, millised andmed ja kui pikk säilitamisaeg on eesmärgi saavutamiseks vajalikud;
    - põhjendamine – vastutav töötleja peab suutma põhjendada, miks säilitamisaeg on eesmärgi saavutamiseks ja kõnealuste isikuandmete puhul vajalik, ning suutma avalikustada säilitamisaja põhjused ja õiguslikud alused;
    - säilitamise põhimõtete jõustamine – vastutav töötleja peab jõustama säilitamise sisekorra ja kontrollima, kas organisatsioon rakendab kehtestatud põhimõtteid;
    - varukoopiad/logid – vastutavad töötlejad peavad kindlaks määrama, millised isikuandmed ja kui pikk säilitamisaeg on varukoopiate ja logide puhul vajalikud;
    - andmevoog – vastutavad töötlejad peaksid olema teadlikud isikuandmete liikumisest ja nende koopiate säilitamisest ning püüdma piirata nende „ajutist“ säilitamist.

Näide

Vastutav töötleja kogub isikuandmeid töötlemistoiminguks, mille eesmärk on hallata andmesubjekti liikmesust. Isikuandmed kustutatakse, kui liikmesus lõpetatakse ja puudub õiguslik alus andmete edasiseks säilitamiseks.

Kõigepealt loob vastutav töötleja sisemenetluse andmete säilitamiseks ja kustutamiseks. Selle kohaselt peavad töötajad pärast säilitamisaja lõppu isikuandmed käsitsi kustutama. Töötaja järgib menetlust

[40] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

kõigis seadmetes, varukoopiatel, logides, e-kirjades ja muudel asjakohastel säilitusmeediumidel leiduvate andmete regulaarseks parandamiseks ning sealt kustutamiseks.

Et muuta kustutamine tõhusamaks ja vähendada eksimusi, hakkab vastutav töötleja selle asemel kasutama automaatsüsteemi, mis võimaldab andmete automaatset ja korrapärasemat kustutamist. Süsteem konfigureeritakse järgima konkreetset andmete kustutamise menetlust, mis seejärel ettemääratud korrapäraste ajavahemike tagant eemaldab isikuandmed kõikidelt ettevõtte säilitamismeediumitelt. Vastutav töötleja vaatab säilitamismenetluse korrapäraselt läbi ja testib seda ning tagab, et see on kooskõlas ajakohaste säilitamispõhimõtetega.

3.8 Terviklus ja konfidentsiaalsus

83. Tervikluse ja konfidentsiaalsuse põhimõte hõlmab kaitset volitamata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid. Isikuandmete turvalisuse tagamiseks on vaja asjakohaseid meetmeid, mille eesmärk on ennetada ja hallata andmetega seotud rikkumisi, tagada andmetöötlusülesannete nõuetekohane täitmine ja muude põhimõtete järgimine ning hõlbustada üksikisikute õiguste tõhusat kasutamist.

84. Põhjenduses 78 on öeldud, et üks lõimitud andmekaitse ja vaikimisi andmekaitse meetmetest võiks hõlmata vastutavale töötlejale võimaluse andmist „luua ja parandada turvameetmeid“. Koos muude lõimitud andmekaitse ja vaikimisi andmekaitse meetmetega tehakse põhjenduses 78 ettepanek panna vastutavatele töötlejatele kohustus pidevalt hinnata, kas kogu aeg kasutatakse nõuetekohaseid töötlemisvahendeid, ja hinnata, kas valitud meetmed aitavad ka tegelikult nõrku kohti korrigeerida. Lisaks peavad vastutavad töötlejad korrapäraselt kontrollima infoturbe meetmeid, mis toetavad ja kaitsevad isikuandmeid, ja rakendama isikuandmetega seotud rikkumiste käsitlemise menetlust.

85. Tervikluse ja konfidentsiaalsuse põhimõtte peamised lõimitud ja vaikimisi andmekaitse aspektid võivad hõlmata järgmist:
    - infoturbe haldamise süsteem – kasutatakse operatiivseid põhimõtete haldamise vahendeid ja infoturbemenetlusi;
    - riskianalüüs – hinnata isikuandmete turbega seotud riske, kaaludes mõju üksikisikute õigustele, ja ohjata tuvastatud riskid. Riskihindamiseks töötada välja terviklik, süstemaatiline ja realistlik ohu modelleerimine ning ründepinna analüüs kavandatud tarkvara kohta ning neid hallata, et vähendada ründevektoreid ning võimalusi kasutada ära nõrku kohti ja turvaauke;
    - lõimitud turvalisus – kaaluda turvanõuete kehtestamist süsteemi kavandamise ja arendamise võimalikult varajases etapis ning pidevalt integreerida ja teha asjakohaseid teste;
    - hooldus – korrapäraselt kontrollida ja testida tarkvara, riistvara, süsteeme ja teenuseid jne, et tuvastada töötlemist toetavate süsteemide nõrgad kohad;
    - juurdepääsukontrolli haldamine – isikuandmetele juurdepääs peaks olema ainult volitatud töötajatel, kellel on neid andmeid vaja oma töötlemisülesannete täitmiseks, ning vastutav töötleja peaks eristama volitatud töötajate juurdepääsuõigusi;
        - juurdepääsupiirang (ametnikud) – kavandada andmete töötlemine nii, et oma ülesannete täitmiseks vajab isikuandmetele juurdepääsu minimaalne arv inimesi, ning vastavalt piirata juurdepääsu;
        - juurdepääsupiirang (sisu) – seoses iga töötlemistoiminguga anda juurdepääs ainult nendele atribuutidele andmekogumis, mida on vaja selle toimingu tegemiseks. Lisaks anda juurdepääs ainult nende andmesubjektide andmetele, kellega asjaomase töötaja tööülesanded on seotud;

    - juurdepääsu eristamine – kavandada andmete töötlemine nii, et ükski isik ei vajaks laiaulatuslikku juurdepääsu kõigile andmesubjekti kohta kogutud andmetele ja kindlasti mitte konkreetse andmesubjektide kategooria kõigile isikuandmetele;
- turvalised edastused – edastused peavad olema kaitstud lubamatu ja juhusliku juurdepääsu ja muutmise eest;
- turvaline säilitamine – andmeid tuleb säilitada nii, et need oleksid kaitstud lubamatu juurdepääsu ja muutmise eest. Tuleks kehtestada menetlused, et hinnata tsentraliseeritud või detsentraliseeritud säilitamise ohtu ja seda, milliseid isikuandmete liike see puudutab. Mõned andmed võivad vajada rohkem turvameetmeid kui teised või neid tuleb hoida teistest eraldi;
- pseudonüümimine – isikuandmed ja varukoopiad/logid tuleks turvameetmena näiteks räsimise või krüptimise teel pseudonüümida, et isikuandmetega seotud võimalike rikkumiste oht oleks minimaalne;
- varukoopiad/logid – hoida varukoopiaid ja logisid infoturbeks vajalikus ulatuses; kasutada korralise turbekontrollina kontrolljälgi ja sündmuste jälgimist. Neid kaitstakse volitamata ja juhusliku juurdepääsu ning muutmise eest ja vaadatakse korrapäraselt läbi, intsidentidega aga tuleb viivitamata tegeleda;
- avariitaaste/talitluspidevus – võtta arvesse infosüsteemide avariitaaste ja talitluspidevuse nõudeid, et taastada pärast suuremaid intsidente isikuandmete kättesaadavus;
- riskipõhine kaitse – kõiki isikuandmete liike tuleks kaitsta turvarikkumise ohu eest piisavate meetmetega. Andmeid, millega kaasnevad erilised ohud, tuleks võimaluse korral hoida muudest isikuandmetest eraldi;
- turvaintsidentidele reageerimise haldamine – rakendada tuleks tegevuskorda, menetlusi ja vahendeid isikuandmetega seotud rikkumiste tuvastamiseks, ohjamiseks, käsitlemiseks, nendest teatamiseks ja õppimiseks;
- intsidendihaldus – vastutaval töötlejal peaksid olema kehtestatud menetlused rikkumiste ja intsidentide käsitlemiseks, et muuta töötlemissüsteem töökindlamaks. See hõlmab teavitamise korda, näiteks järelevalveasutusele teatamise ja andmesubjektide teavitamise haldamist.

Näide

Vastutav töötleja soovib teha suurtes kogustes isikuandmete väljavõtte meditsiiniandmebaasist, mis sisaldab elektroonilisi (patsientide) terviseandmeid, ja salvestada need ettevõtte spetsiaalsesse andmebaasiserverisse, et töödelda väljavõetud andmeid kvaliteedi tagamise eesmärgil. Ettevõte leidis hindamise käigus, et andmeväljavõtete üleviimine serverisse, mis on ligipääsetav ettevõtte kõikidele töötajatele, kujutab endast tõenäoliselt suurt ohtu andmesubjekti õigustele ja vabadustele. Kuna ettevõttes on ainult üks osakond, kes peab patsiendiandmete väljavõtteid töötlema, otsustab vastutav töötleja anda spetsiaalsele serverile juurdepääsu ainult selle osakonna töötajatele. Et riski veelgi vähendada, pseudonüümitakse andmed enne edastamist.

Juurdepääsu reguleerimiseks ja pahavarast põhjustatud võimaliku kahju vähendamiseks otsustab ettevõte võrgu eraldada ning kehtestada serverile juurdepääsu kontrolli. Lisaks võetakse kasutusele turvaseire ning sissetungi tuvastamise ja ennetamise süsteem, millele tavakasutajad ligi ei pääse. Juurdepääsu ja muudatuste jälgimiseks võetakse kasutusele automatiseeritud auditeerimissüsteem. See loob aruanded ja automaatsed hoiatused, kui konfigureeritakse kasutusega seotud teatud sündmused. Vastutav töötleja tagab, et kasutajatel on juurdepääs teadmisvajaduse põhimõttel ja asjakohasel juurdepääsutasemel. Asjakohatut kasutust saab kiiresti ja hõlpsasti tuvastada.

Mõningaid väljavõtteid tuleb võrrelda uute väljavõtetega ning neid tuleb seetõttu säilitada kolm kuud. Vastutav töötleja otsustab panna need samasse serverisse eraldi andmebaasidesse ning kasutada

nende salvestamiseks nii läbipaistvat kui ka veeru tasandi krüpteerimist. Veeru andmete dekrüpteerimise võtmed salvestatakse spetsiaalsetesse turvamoodulitesse, mida saavad kasutada üksnes volitatud töötajad ning millest ei ole võimalik teha väljavõtteid.

Tulevaste intsidentide käsitlemine muudab süsteemi töökindlamaks ja usaldusväärsemaks. Vastutav andmetöötleja mõistab, et ennetavad ja tõhusad meetmed ning kaitsemeetmed tuleb lõimida kogu praegusesse ja tulevasse isikuandmete töötlemise protsessi ning et nii toimimine võib aidata edaspidi sellised isikuandmetega seotud rikkumise juhtumid ära hoida.

Vastutav töötleja kehtestab need turvameetmed nii õigsuse, terviklikkuse ja konfidentsiaalsuse tagamiseks kui ka küberrünnetel põhineva pahavara leviku ärahoidmiseks, et muuta lahendus kindlaks. Tugevate turvameetmete olemasolu aitab suurendada andmesubjektide usaldust.

3.9 Vastutus[41]

86. Vastutuse põhimõtte kohaselt vastutab vastutav töötleja kõigi eespool nimetatud põhimõtete täitmise eest ja peab olema suuteline seda tõendama.

87. Vastutav töötleja peab suutma tõendada, et põhimõtteid järgitakse. Seejuures võib vastutav töötleja tõendada andmesubjektide õiguste kaitseks võetud meetmete mõju ning seda, miks neid meetmeid peetakse asjakohasteks ja tõhusateks. Näiteks võib ta näidata, miks meede on asjakohane, et tagada tõhusalt säilitamise piirangu põhimõtte järgimine.

88. Selleks et vastutav töötleja saaks isikuandmeid vastutustundlikult töödelda, peaksid tal olema nii teadmised andmekaitse rakendamise kohta kui ka suutlikkus seda teha. See tähendab, et vastutav töötleja peaks mõistma oma andmekaitsekohustusi, mis on ette nähtud isikuandmete kaitse üldmäärusega, ja olema võimeline neid täitma.

4 ARTIKLI 25 LÕIGE 3: SERTIFITSEERIMINE

89. Artikli 25 lõike 3 kohaselt võib lõimitud andmekaitse ja vaikimisi andmekaitse nõuete järgimise tõendamise elemendina kasutada artikli 42 kohast sertifitseerimist. Samas võib dokumentidest, mis tõendavad vastavust lõimitud ja vaikimisi andmekaitse nõuetele, olla kasu ka sertifitseerimisprotsessis. See tähendab, et kui vastutava töötleja või volitatud töötleja töötlemistoiming on sertifitseeritud kooskõlas artikliga 42, võtavad järelevalveasutused seda arvesse isikuandmete kaitse üldmääruse järgimise hindamisel, eelkõige lõimitud ja vaikimisi andmekaitse kontekstis.

90. Kui vastutava töötleja või volitatud töötleja töötlemistoiming on sertifitseeritud kooskõlas artikliga 42, on elemendid, mis aitavad tõendada vastavust artikli 25 lõigetele 1 ja 2, kavandamisprotsessid, st töötlemisvahendite kindlaksmääramise protsess, juhtimine ning tehnilised ja korralduslikud meetmed andmekaitse põhimõtete rakendamiseks. Andmekaitse sertifitseerimise kriteeriumid määravad kindlaks sertifitseerimisasutused või sertifitseerimissüsteemi valdajad ning seejärel kiidab need heaks pädev järelevalveasutus või Euroopa Andmekaitsenõukogu. Lisateavet sertifitseerimismehhanismide kohta leiate Euroopa Andmekaitsenõukogu sertifitseerimissuunistest[42] ja muudest asjakohastest juhistest, mis on avaldatud Euroopa Andmekaitsenõukogu veebisaidil.

[41] Vt põhjendus 74, mille kohaselt peavad vastutavad töötlejad tõendama oma meetmete tõhusust.
[42] Euroopa Andmekaitsenõukogu suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta. Versioon 3.0, 4. juuni 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_et.pdf.

91. Isegi kui töötlemistoimingule antakse artikli 42 kohane sertifikaat, on vastutaval töötlejal endiselt kohustus pidevalt jälgida ja parandada vastavust artiklis 25 sätestatud lõimitud ja vaikimisi andmekaitse kriteeriumidele.

5 ARTIKLI 25 JÕUSTAMINE JA TAGAJÄRJED

92. Järelevalveasutused võivad hinnata vastavust artiklile 25 kooskõlas artiklis 58 loetletud menetlustega. Parandusvolitused on määratletud artikli 58 lõikes 2 ning need hõlmavad hoiatuste ja noomituste tegemist ning korralduste andmist andmesubjekti õiguste, töötlemise piirangute või keelu, haldustrahvide jms järgimiseks.

93. Lõimitud andmekaitse ja vaikimisi andmekaitse on lisaks tegur isikuandmete kaitse üldmääruse rikkumistega seotud rahaliste karistuste suuruse määramisel – vt artikli 83 lõiget 4[43] [44].

6 SOOVITUSED

94. Kuigi volitatud töötlejaid ja tootjaid ei ole artiklis 25 otseselt käsitletud, on ka neil lõimitud ja vaikimisi andmekaitse tagamisel tähtis roll ja nad peaksid olema teadlikud sellest, et vastutavad töötlejad on kohustatud töötlema isikuandmeid üksnes süsteemide ja tehnoloogiate abil, mille lahutamatu osa on andmekaitse.

95. Vastutavate töötlejate nimel töötlemise või vastutavatele töötlejatele lahenduste pakkumise korral peaksid volitatud töötlejad ja tootjad kasutama oma kogemusi, et suurendada usaldust ja suunata oma kliente, sh VKEsid, kavandades ja hankides lahendusi, mille puhul töötlemisprotsess hõlmab ka andmekaitset. See omakorda tähendab, et kavandatavad tooted ja teenused peaksid hõlbustama vastutavate töötlejate vajaduste rahuldamist.

96. Artikli 25 rakendamisel tuleb meeles pidada, et töötlemise kavandamisel on peamine eesmärk, et asjakohaste töötlemismeetmetega oleks tagatud põhimõtete *tõhus rakendamine* ja andmesubjektide õiguste *kaitse*. Selleks et hõlbustada ja edendada lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete järgimist, on järgnevalt esitatud soovitused vastutavatele töötlejatele, tootjatele ja volitatud töötlejatele.
    - Vastutavad töötlejad peavad mõtlema andmekaitsele alates töötlemistoimingu kavandamise *algetappidest*, isegi enne töötlemisvahendite kindlaksmääramist.
    - Kui vastutaval töötlejal on andmekaitseametnik, julgustab andmekaitsenõukogu andmekaitseametnikku aktiivselt osalema lõimitud ja vaikimisi andmekaitse integreerimisel hanke- ja arendusmenetlustesse ning kogu töötlemistsüklisse.
    - Töötlemistoimingu võib *sertifitseerida*. Kui töötlemistoiming õnnestub sertifitseerida, annab see vastutavale töötlejale lisaväärtust, kui ta valib tootjate või volitatud töötlejate eri töötlemistarkvara, -riistvara, -teenuste ja/või -süsteemide vahel. Seepärast peaksid tootjad

[43] Isikuandmete kaitse üldmääruse artikli 83 lõike 2 punktis d on sätestatud, et isikuandmete kaitse üldmääruse rikkumiste eest trahvide määramisel pööratakse asjakohast tähelepanu vastutava töötleja või volitatud töötleja vastutuse astmele, võttes arvesse nende poolt artiklite 25 ja 32 kohaselt võetud tehnilisi ja korralduslikke meetmeid.

[44] Lisateave trahvide kohta on saadaval artikli 29 töörühma dokumendis „Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta“. WP 253, 3. oktoober 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 – kinnitanud Euroopa Andmekaitsenõukogu.

püüdma tõendada lõimitud ja vaikimisi andmekaitse põhimõtete järgimist kogu töötlemislahenduse väljatöötamise protsessis. Sertifitseerimispitser võib samuti aidata andmesubjektidel valida eri kaupade ja teenuste vahel. Suutlikkus töötlemistoiming sertifitseerida võib seega olla tootjate, volitatud töötlejate ja vastutavate töötlejate jaoks konkurentsieelis ning suurendab ka andmesubjektide usaldust nende isikuandmete töötlemise vastu. Kui sertifitseerimisvõimalus puudub, peaksid vastutavatel töötlejatel olema muud *tagatised* selle kohta, et tootjad ja volitatud töötlejad järgivad lõimitud andmekaitse ja vaikimisi andmekaitse nõudeid.

- Vastutavad töötlejad, volitatud töötlejad ja tootjad peaksid võtma arvesse oma kohustust pakkuda alla 18-aastastele lastele ja teistele haavatavatele rühmadele lõimitud ja vaikimisi andmekaitse nõuete täitmisel erikaitset.
- Tootjad ja volitatud töötlejad peaksid püüdma hõlbustada lõimitud ja vaikimisi andmekaitse rakendamist, et aidata vastutaval töötlejal täita artiklis 25 sätestatud kohustusi. Samas ei tohiks vastutavad töötlejad valida tootjaid ega volitatud töötlejaid, kes ei paku süsteeme, mis võimaldaksid või aitaksid vastutaval töötlejal järgida artiklit 25, kuna vastutus selle artikli täitmata jätmise eest lasub vastutavatel töötlejatel.
- Tootjad ja volitatud töötlejad peaksid täitma aktiivset osa teaduse ja tehnika viimase arengu kriteeriumide täitmise tagamisel ning teavitama vastutavaid töötlejaid teaduse ja tehnika viimase arengu mis tahes muutustest, mis võivad mõjutada kasutusele võetud meetmete tõhusust. Vastutavad töötlejad peavad lisama selle nõude lepingutingimusena, et kindlustada nende ajakohastena hoidmine.
- Euroopa Andmekaitsenõukogu soovitab vastutavatel töötlejatel nõuda, et tootjad ja volitatud töötlejad näitaksid, kuidas nende riistvara, tarkvara, teenused või süsteemid võimaldavad vastutaval töötlejal täita vastutuse nõudeid kooskõlas lõimitud ja vaikimisi andmekaitse põhimõtetega, näiteks tõendades tulemuslikkuse põhinäitajate abil, et meetmed ja kaitsemeetmed on põhimõtete ja õiguste rakendamiseks tõhusad.
- Euroopa Andmekaitsenõukogu rõhutab, et põhimõtete ja õiguste tõhusaks rakendamiseks on vaja ühtlustatud käsitlust, ning innustab ühendusi ja asutusi artikli 40 kohaste toimimisjuhendite koostamisel lisama nendesse ka valdkonnapõhised suunised lõimitud ja vaikimisi andmekaitse kohta.
- Vastutavad töötlejad peavad olema andmesubjektide suhtes ausad ja läbipaistvad selles, kuidas nad hindavad ja tõendavad lõimitud ja vaikimisi andmekaitse tõhusat rakendamist, samuti nagu vastutavad töötlejad tõendavad vastavust isikuandmete kaitse üldmäärusele vastutuse põhimõtte alusel.
- Eraelu puutumatust soodustavaid tehnoloogiaid, mis on saavutanud tipptasemel küpsuse, võib kasutada meetmena kooskõlas lõimitud ja vaikimisi andmekaitse nõuetega, kui see on riskipõhisest lähenemisviisist lähtudes asjakohane. Eraelu puutumatust soodustavad tehnoloogiad ei taga iseenesest artiklis 25 sätestatud kohustuste täitmist. Vastutavad töötlejad hindavad, kas meede on andmekaitsepõhimõtete ja andmesubjektide õiguste rakendamisel asjakohane ja tõhus.
- Olemasolevate varasemate süsteemide suhtes kehtivad samad lõimitud ja vaikimisi andmekaitse kohustused nagu uute suhtes. Kui varasemad süsteemid ei vasta juba lõimitud ja vaikimisi andmekaitse nõuetele ning kohustuste täitmiseks ei ole võimalik muudatusi teha, siis ei taga vana süsteem isikuandmete kaitse üldmäärusest tulenevate kohustuste täitmist ja seda ei saa kasutada isikuandmete töötlemiseks.

- Artikliga 25 ei ole VKEdele kehtestatud leebemaid nõudeid. Järgmised nõuanded võivad muuta VKEdel artikli 25 järgimise lihtsamaks.
    - Tehke riskihindamine varakult
    - Alustage väikesemahulisest töötlemisest ning hiljem laiendage selle ulatust ja keerukust
    - Uurige, kas tootjatel ja volitatud töötlejatel on tagatised selle kohta, et nad rakendavad lõimitud ja vaikimisi andmekaitset, näiteks sertifikaat ja toimimisjuhendi järgimine
    - Kasutage hea hinnangu saanud partnereid
    - Rääkige andmekaitseasutustega
    - Lugege andmekaitseasutuste ja Euroopa Andmekaitsenõukogu suuniseid
    - Kui on olemas toimimisjuhendid, siis järgige neid
    - Küsige abi ja nõu professionaalidelt

Euroopa Andmekaitsenõukogu nimel

Eesistuja

(Andrea Jelinek)