Suunised

Suunised 9/2022, mis käsitlevad isikuandmetega seotud rikkumisest teatamist isikuandmete kaitse üldmääruse alusel

Versioon 2.0

Vastu võetud 28. märtsil 2023

Versioonid

Versioon 1.0	10. oktoober 2022	Suuniste (eelmiste suuniste WP250 rev.01 (mille võttis vastu artikli 29 töörühm ja mille Euroopa Andmekaitsenõukogu kiitis heaks 25. mail 2018) ajakohastatud versioon) vastuvõtmine sihitatud avalikuks konsultatsiooniks.
Versioon 2.0	28. märts 2023	Suuniste vastuvõtmine pärast sihitatud avalikku konsultatsiooni, milles käsitleti isikuandmetega seotud rikkumistest teatamist väljaspool EMPd asuvate vastutavate töötlejate puhul.

SISUKORD

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (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 punkte e ja l,

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[1],

võttes arvesse oma kodukorra artiklit 12 ja artiklit 22,

võttes arvesse artikli 29 töörühma suuniseid, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel (WP 250 rev.01),

ON VASTU VÕTNUD JÄRGMISED SUUNISED.

0 EESSÕNA

1. 3. oktoobril 2017 võttis artikli 29 töörühm vastu suunised, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel (WP 250 rev.01),[2] mille Euroopa Andmekaitsenõukogu kiitis heaks oma esimesel täiskogu istungil[3]. Käesolev dokument on suuniste pisut ajakohastatud versioon. Kõiki viiteid artikli 29 töörühma suunistele, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel (WP 250 rev.01), tuleks edaspidi tõlgendada viidetena Euroopa Andmekaitsenõukogu suunistele 9/2022.

2. Euroopa Andmekaitsenõukogu märkis, et vaja on anda selgitusi rikkumisest teatamise nõuete kohta, mis puudutavad isikuandmetega seotud rikkumisi kolmandates riikides. Seda küsimust käsitlev punkt on läbi vaadatud ja seda on ajakohastatud. Ülejäänud dokumenti muudetud ei ole, kui toimetuslikud muudatused välja arvata. Täpsemalt puudutab läbivaatamine käesoleva dokumendi jao II.C.2 punkti 73.

SISSEJUHATUS

3. Isikuandmete kaitse üldmäärusega kehtestati nõue teavitada pädevat riiklikku järelevalveasutust[4] (või piiriülese rikkumise korral juhtivat järelevalveasutust) isikuandmetega seotud rikkumisest (edaspidi „rikkumine“) ja teatavatel juhtudel teavitada rikkumisest ka üksikisikuid, kelle isikuandmeid on rikkumine mõjutanud.

4. Rikkumisest teatamise kohustus oli varem teatud asutustel, näiteks üldkasutatavate elektrooniliste sideteenuste osutajatel (nagu on täpsustatud direktiivis 2009/136/EÜ ja määruses (EL) nr 611/2013)[5].

---

[1] Kõiki käesolevas dokumendis sisalduvaid viiteid liikmesriikidele tuleks käsitada viidetena EMP liikmesriikidele.
[2] Artikli 29 töörühma suunised, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel (WP 250 rev.01) (viimati muudetud ja ajakohastatud 6. veebruaril 2018), kättesaadavad aadressil https://ec.europa.eu/newsroom/article29/items/612052.
[3] Vt https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] Vt isikuandmete kaitse üldmääruse artikli 4 punkt 21.
[5] Vt http://eur-lex.europa.eu/legal-content/ET/XT/?uri=celex:32009L0136 ja http://eur-lex.europa.eu/legalcontent/ET/XT/?uri=CELEX%3A32013R0611

Mõnes liikmesriigis oli juba kehtestatud ka riigisisene rikkumisest teatamise kohustus. Tegemist võis olla kohustusega teavitada rikkumisest, millega on seotud vastutavate töötlejate kategooriad lisaks üldkasutatavate elektroonilise side teenuste osutajatele (näiteks Saksamaal ja Itaalias), või kohustusega teatada kõikidest isikuandmetega seotud rikkumistest (näiteks Hollandis). Teistel liikmesriikidel võisid olla kasutusel vastavad tegevusjuhised (näiteks Iirimaa[6]). Ehkki mitmed ELi andmekaitseasutused julgustasid vastutavaid töötlejaid rikkumistest teatama, ei olnud andmekaitsedirektiivis 95/46/EÜ,[7] mis asendati isikuandmete kaitse üldmäärusega, konkreetset kohustust rikkumisest teatada ning seega oli selline nõue paljudele organisatsioonidele uus. Isikuandmete kaitse üldmäärusega muudetakse rikkumisest teatamine kõikide vastutavate töötlejate jaoks kohustuslikuks, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ega vabadustele[8]. Ka volitatud töötlejatel on oluline roll ja nemad peavad teavitama kõikidest rikkumistest vastutavat töötlejat[9].

5. Euroopa Andmekaitsenõukogu leiab, et rikkumisest teatamise nõudel on mitmeid eeliseid. Järelevalveasutuse teavitamisel saavad vastutavad töötlejad küsida nõu, kas mõjutatud üksikisikuid tuleb teavitada. Järelevalveasutus võib tõepoolest anda vastutavale töötlejale korralduse teavitada rikkumisest ka asjaomaseid üksikisikuid[10]. Üksikisikute teavitamine võimaldab vastutaval töötlejal edastada teavet rikkumise tulemusel tekkinud ohtude kohta, samuti sammude kohta, mida need üksikisikud saavad astuda, et kaitsta ennast võimalike tagajärgede eest. Iga rikkumisele reageerimise plaani peamine eesmärk peaks olema kaitsta üksikisikuid ja nende isikuandmeid. Sellest tulenevalt tuleks rikkumisest teatamist näha kui vahendit, millega tõhustada isikuandmete kaitsega seotud nõuete täitmist. Samas olgu märgitud, et rikkumisest üksikisikule või järelevalveasutusele teatamata jätmine võib tähendada, et vastutavale töötajale võidakse isikuandmete kaitse üldmääruse artikli 83 alusel määrata karistus.

6. Vastutavaid töötlejaid ja volitatud töötlejaid julgustatakse seetõttu tegema ettevalmistusi ja kehtestama protsesse, et olla suuteline rikkumisi avastama, need koheselt peatama ja hindama üksikisikutele avalduvat ohtu,[11] ning seejärel tegema kindlaks, kas pädevat järelevalveasutust on vaja teavitada, ning vajaduse korral teavitama rikkumisest asjaomaseid üksikisikuid. Järelevalveasutuste teavitamine peaks olema intsidentidele reageerimise plaani osa.

7. Isikuandmete kaitse üldmäärus sisaldab sätteid selle kohta, millal ja keda tuleb rikkumisest teavitada ning millist teavet tuleb edastada. Teatamiseks vajaliku teabe võib esitada järk-järgult, kuid igal juhul peavad vastutavad töötajad tegutsema iga rikkumise korral õigeaegselt.

8. Oma arvamuses 03/2014 isikuandmetega seotud rikkumistest teatamise kohta[12] esitas artikli 29 töörühm vastutavatele töötlejatele juhised, mille alusel nad saavad otsustada, kas andmesubjekte teavitada rikkumisest. Selles arvamuses käsitleti direktiivi 2002/58/EÜ elektrooniliste sideteenuste osutajate teavitamise kohustust ning sel ajal eelnõu staadiumis olnud isikuandmete kaitse üldmääruse

---

[6] Vt https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Vt http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:31995L0046

[8] ELi põhiõiguste hartas sätestatud õigused, http://eurlex.europa.eu/legal-content/ET/TXT/?uri=CELEX:12012P/TXT

[9] Vt isikuandmete kaitse üldmääruse artikli 33 lõige 2. See on sarnane määruse (EL) nr 611/2013 artikliga 5, milles on ette nähtud, et teenuseosutaja, kes osutab allhanke korras osa elektroonilisest sideteenusest (ilma et ta oleks abonentidega otseses lepingulises suhtes), teavitab isikuandmetega seotud rikkumise korral kohe allhankivat teenuseosutajat.

[10] Vt isikuandmete kaitse üldmääruse artikli 34 lõige 4 ja artikli 58 lõike 2 punkt e.

[11] Seda saab tagada andmekaitsealasest mõjuhinnangust tuleneva järelevalve ja läbivaatamise nõude alusel, mida tuleb kohaldada selliste töötlemistoimingute puhul, mille tagajärjel tekib füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht (artikli 35 lõiked 1 ja 11).

[12] Vt artikli 29 töörühma arvamus 03/2014 isikuandmetega seotud rikkumistest teatamise kohta http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_et.pdf

valguses esitati näiteid erinevatest valdkondadest ja parimaid tavasid kõikide vastutavate töötlejate jaoks.

9. Käesolevates suunistes selgitatakse isikuandmete kaitse üldmäärusest tulenevaid kohustuslikke rikkumisest teatamise ja teabe edastamise nõudeid ning mõningaid samme, mida vastutavad töötlejad ja volitatud töötlejad saavad oma kohustuste täitmiseks teha. Samuti esitatakse näiteid erinevate rikkumiste kohta ning selle kohta, keda tuleks erinevates olukordades teavitada.

I. ISIKUANDMETEGA SEOTUD RIKKUMISEST TEATAMINE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ALUSEL

A. Peamised turvakaalutlused

10. Isikuandmete kaitse üldmääruse üks nõuetest on, et isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid[13].

11. Sellest tulenevalt nõutakse isikuandmete kaitse üldmääruses, et nii vastutavad töötlejad kui ka volitatud töötlejad kehtestavad ohule vastava turvalisuse taseme tagamiseks asjakohased tehnilised ja korralduslikud meetmed. Neil tuleks võtta arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja tõsidusega ohte füüsiliste isikute õigustele ja vabadustele[14]. Samuti nõutakse isikuandmete kaitse üldmääruses kõikide asjakohaste tehniliste kaitsemeetmete ja korralduslike meetmete kehtestamist, et teha viivitamata kindlaks, kas rikkumine on toimunud, mis omakorda määrab kindlaks, kas on tekkinud teatamiskohustus[15].

12. Sellest tulenevalt on iga andmeturbepoliitika üks võtme tegureid suutlikkus rikkumisi võimaluse korral ära hoida ja kui need siiski esinevad, reageerida neile õigeaegselt.

B. Mis on isikuandmetega seotud rikkumine?

1. Mõiste

13. Selleks et vastutav töötleja saaks rikkumisega tegeleda, tuleks tal see esmalt ära tunda. Isikuandmete kaitse üldmääruse artikli 4 punktis 12 on „isikuandmetega seotud rikkumine“ määratletud järgmiselt:

> „turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.“

14. See, mida mõeldakse isikuandmete „hävitamise“ all, peaks olema üsna selge: see on olukord, kus andmeid enam ei eksisteeri või ei eksisteeri sellises vormingus, mida vastutav töötleja saaks kasutada. Ka „kahju“ mõiste peaks olema võrdlemisi selge: olukord, kus isikuandmeid on muudetud, rikutud või need ei ole enam terviklikud. Isikuandmete „kaotsiminekut“ võib tõlgendada kui olukorda, kus andmed on endiselt olemas, kuid vastutaval töötlejal ei ole nende üle enam kontrolli või nendele juurdepääsu või ei ole andmed enam tema valduses. Loata või ebaseaduslik töötlemine võib tähendada ka seda, et isikuandmeid avaldavad (või võimaldavad nendele juurdepääsu) isikud, kellel ei ole luba neid andmeid vastu võtta (või nendele juurde pääseda), või töödeldakse andmeid mis tahes muul viisil, mis rikub isikuandmete kaitse üldmäärust.

---

[13] Vt isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt f ja artikkel 32.

[14] Artikkel 32; vt ka isikuandmete kaitse üldmääruse põhjendus 83.

[15] Vt isikuandmete kaitse üldmääruse põhjendus 87.

Näide

Isikuandmete kaotsiminek on toimunud näiteks siis, kui seade, kuhu on salvestatud vastutava töötleja klientide andmebaas, on kaotatud või varastatud. Teine näide kaotsiminekust on olukord, kus isikuandmeid sisaldav ainukoopia on lunavara abil krüpteeritud või vastutav töötleja on koopia krüpteerinud võtmega, mis enam ei ole tema valduses.

15. Tuleks rõhutada, et rikkumine on turvaintsidendi üks liikidest. Kuid nagu on osutatud artikli 4 punktis 12, kohaldatakse isikuandmete kaitse üldmäärust üksnes juhul, kui rikkumine on seotud isikuandmetega. Sellise rikkumise tagajärjel ei suuda vastutav töötleja tagada vastavust isikuandmete kaitse üldmääruse artiklis 5 loetletud isikuandmete töötlemise põhimõtetega. Siit tuleb välja erinevus turvaintsidendi ja isikuandmetega seotud rikkumise vahel – kuigi sisuliselt on kõik isikuandmetega seotud rikkumised turvaintsidendid, ei ole kõik turvaintsidendid tingimata isikuandmetega seotud rikkumised[16].

16. Rikkumise võimalikku kahjulikku mõju üksikisikutele arutatakse allpool.

2. Isikuandmetega seotud rikkumiste liigid

17. Artikli 29 töörühm selgitas oma arvamuses 03/2014 rikkumisest teatamise kohta, et rikkumised võib jaotada kategooriatesse vastavalt järgmisele kolmele tuntud infoturbe põhimõttele[17]:

- **„konfidentsiaalsusega seotud rikkumine“** – isikuandmete loata või juhuslik avalikustamine või neile juurdepääs;
- **„terviklusega seotud rikkumine“** – isikuandmete loata või juhuslik muutmine;
- **„kättesaadavusega seotud rikkumine“** – isikuandmetele juurdepääsu juhuslik või loata kadumine[18] või isikuandmete hävitamine.

18. Samuti tuleb märkida, et olenevalt olukorrast võib rikkumine olla ühtaegu seotud nii isikuandmete konfidentsiaalsuse, tervikluse kui ka kättesaadavusega või kombinatsioonina nendest.

19. Kui konfidentsiaalsuse või terviklusega seotud rikkumise kindlaksmääramine on suhteliselt selge, siis kättesaadavusega seotud rikkumise kindlaksmääramine ei pruugi nii ilmne olla. Rikkumist peetakse alati kättesaadavusega seotud rikkumiseks, kui isikuandmed on püsivalt kadunud või hävitatud.

Näide

Kättesaadavuse kadumise näidete hulka kuulub olukord, kus andmed on kogemata kustutatud või need on kustutanud volitamata isik või kui turvaliselt krüpteeritud andmete võti on kaduma läinud. Juhul, kui vastutav töötaja ei suuda taastada juurdepääsu andmetele, näiteks varukoopia abil, peetakse seda kättesaadavuse püsivaks kadumiseks.

[16] Olgu märgitud, et turvaintsident ei piirdu ohumudelitega, kus organisatsiooni rünnatakse välisest allikast, vaid see hõlmab ka asutusesisesest töötlemisest tulenevaid intsidente, millega rikutakse turvalisuse põhimõtteid.
[17] Vt artikli 29 töörühma arvamus 03/2014.
[18] Üldise arusaama kohaselt on „juurdepääs“ põhimõtteliselt osa „kättesaadavusest“. Vt näiteks NIST SP800-SP80053rev4, kus „kättesaadavus“ on määratletud järgmiselt: „Teabele õigeaegse ja usaldusväärse juurdepääsu ja selle kasutamise tagamine“, kättesaadav aadressil http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Ka dokumendis CNSSI-4009 mõeldakse kättesaadavuse all volitatud kasutajate õigeaegset ja usaldusväärset juurdepääsu andmetele ning teabeteenustele. Vt https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 standardis on „kättesaadavus“ samuti määratletud kui „teave, millele volitatud üksusel on juurdepääs ja mida ta saab nõudmise korral kasutada“: https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

Kättesaadavuse kadumine võib esineda ka siis, kui organisatsiooni tavapärases toimimises on toimunud märkimisväärne katkestus, näiteks elektrikatkestus või teenusetõkestusrünne, mis muudab isikuandmed kättesaamatuks.

20. Võib küsida, kas isikuandmete ajutist kättesaadavuse kadumist võib pidada rikkumiseks, ning kui saab, siis kas sellest tuleb teatada. Isikuandmete kaitse üldmääruse artiklis 32 „Töötlemise turvalisus“ on täpsustatud, et kui rakendatakse tehnilisi ja korralduslikke meetmeid, et tagada ohule vastav turvalisuse tase, tuleks muu hulgas arvestada „võimega tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus“ ja „võimega taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral“.

21. Seega on turvaintsident, mille tõttu ei ole isikuandmed teatud aja jooksul kättesaadavad, samuti rikkumine, kuna andmetele juurdepääsu puudumine võib märkimisväärselt mõjutada füüsiliste isikute õigusi ja vabadusi. Selguse huvides olgu öeldud, et kui isikuandmed ei ole kättesaadavad kavandatud süsteemihoolduse tõttu, ei ole see turvanõuete rikkumine, nagu see on määratletud isikuandmete kaitse üldmääruse artikli 4 punktis 12.

22. Kui isikuandmete kadumine või hävitamine on püsiv (või kui tegemist on ka ükskõik millise muu rikkumisega), tuleb kättesaadavuse ajutine kadumine dokumenteerida kooskõlas isikuandmete kaitse üldmääruse artikli 33 lõike 5 nõuetega. See aitab vastutaval töötlejal täita oma vastutuskohustust järelevalveasutuse ees, kes võib nõuda neid dokumente[19] näha. Kuid see, kas järelevalveasutuse teavitamine ning mõjutatud isikutele teabe edastamine on vajalik või tarbetu, oleneb rikkumise asjaoludest. Vastutav töötleja peab hindama, kui tõenäoliselt ja tõsiselt mõjutab isikuandmete kättesaadavuse puudumine füüsiliste isikute õigusi ja vabadusi. Kooskõlas isikuandmete kaitse üldmääruse artikliga 33 peab vastutav töötleja rikkumisest teatama, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ega vabadustele. Kahtlemata tuleb olukorda hinnata iga juhtumi puhul eraldi.

Näide

Kui haiglas ei ole patsientide kriitilised terviseandmed kasvõi ajutiselt kättesaadavad, võib see kujutada endast ohtu üksikisikute õigustele ja vabadustele. Näiteks võidakse operatsioone ära jätta, mis seaksid inimeste elusid ohtu.

Seevastu kui meediaettevõtte süsteemid ei ole mitme tunni jooksul kättesaadavad (nt elektrikatkestuse tõttu) ja ettevõte ei saa seetõttu oma tellijatele uudiskirja saata, ei kujuta see üksikisikute õigustele ega vabadustele tõenäoliselt ohtu.

23. Olgu märgitud, et ehkki vastutava töötaja süsteemide kättesaadavuse kadumine võib olla ajutine ja ei pruugi mõjutada üksikisikuid, on oluline, et vastutav töötleja kaalub kõiki rikkumise võimalikke tagajärgi, sest teavitamine võib olla vajalik mõnel muul põhjusel.

Näide

Lunavaraga (pahavara, mis krüpteerib vastutava töötleja andmed kuni lunaraha maksmiseni) nakatumine võib põhjustada kättesaadavuse ajutise kadumise, kui andmeid on võimalik taastada varukoopiast. Kuid võrku on siiski sisse tungitud ja teavitamine võib olla vajalik, kui intsidenti saab käsitada konfidentsiaalsusega seotud rikkumisena (st ründaja pääseb isikuandmetele juurde) ning see seab üksikisikute õigused ja vabadused ohtu.

[19] Vt isikuandmete kaitse üldmääruse artikli 33 lõige 5.

3. Isikuandmetega seotud rikkumise võimalikud tagajärjed

24. Rikkumine võib avaldada üksikisikutele märkimisväärset kahjulikku mõju mitmel viisil ja selle tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju. Isikuandmete kaitse üldmääruses on selgitatud, et see võib hõlmata kontrolli kaotamist oma isikuandmete üle, õiguste piiramist, diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, pseudonümiseerimise loata tühistamist, maine kahjustamist ja ametisaladusega kaitstud andmete konfidentsiaalsuse kadu. Samuti võib see hõlmata muud märkimisväärset majanduslikku või sotsiaalset kahju asjaomastele füüsilistele isikutele[20].

25. Seetõttu nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja teavitab rikkumisest pädevat järelevalveasutust, välja arvatud juhul, kui rikkumisest tuleneva kahjuliku mõju oht on ebatõenäoline. Kui kahjuliku mõju oht on tõenäoliselt suur, nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja teavitab rikkumisest mõjutatud üksikisikuid nii kiiresti kui mõistlikkuse piires võimalik[21].

26. Isikuandmete kaitse üldmääruse artiklis 87 on rõhutatud, kui oluline on suuta rikkumine tuvastada, hinnata selle ohtu üksikisikutele ja sellest vajaduse korral teavitada:

> „Tuleks kontrollida, kas kõiki asjakohaseid tehnilisi kaitsemeetmeid ja korralduslikke meetmeid on rakendatud, et teha viivitamata kindlaks, kas isikuandmetega seotud rikkumine on toimunud, ning teavitada sellest kohe järelevalveasutust ning andmesubjekti. Asjaolu, et teavitamine toimus põhjendamatu viivituseta, tuleks kindlaks teha, arvestades eelkõige isikuandmetega seotud rikkumise laadi, tõsidust ja tagajärgi ning kahjulikku mõju andmesubjektile. Sellise teavitamise järel võib asjasse sekkuda järelevalveasutus, kooskõlas talle käesolevas määruses ette nähtud ülesannete ja volitustega.“

27. Täiendavaid suuniseid üksikisikutele avalduvast kahjulikust mõjust tuleneva ohu hindamise kohta käsitletakse IV jaos.

28. Kui vastutavad töötlejad ei teata andmete rikkumisest ei järelevalveasutusele ega andmesubjektidele, olgugi et isikuandmete kaitse üldmääruse artikli 33 ja/või 34 nõuded on täidetud, tuleb järelevalveasutusel kaaluda kõiki tema käsutuses olevaid parandusmeetmeid ja sealhulgas kaaluda vajadust määrata asjakohane trahv[22] kas koos isikuandmete kaitse üldmääruse artikli 58 lõike 2 kohase parandusmeetmega või eraldi. Kui otsustatakse määrata trahv, võib selle suurus isikuandmete kaitse üldmääruse artikli 83 lõike 4 punkti a kohaselt olla kuni 10 000 000 eurot või ettevõtja puhul kuni 2 % tema ülemaailmsest aastasest kogukäibest. Samuti on oluline pidada meeles, et teatud juhtudel võib rikkumisest teatamata jätmine näidata, et turvameetmed puuduvad või et kehtivad turvameetmed on puudulikud. Artikli 29 töörühma suunistes on trahvide kohta öeldud järgmist: „Kui ühe konkreetse juhtumi puhul on toime pandud mitu erinevat rikkumist, siis tähendab see seda, et järelevalveasutus saab kohaldada trahve tasemel, mis on tõhus, proportsionaalne ja heidutav kõige raskema rikkumise seisukohast.“ Sellisel juhul on järelevalveasutusel võimalus määrata karistus ühelt poolt rikkumisest teatamata jätmise eest (isikuandmete kaitse üldmääruse artiklid 33 ja 34) ja teiselt poolt (piisavate) turvameetmete puudumise eest (isikuandmete kaitse üldmääruse artikkel 32), kuna tegemist on kahe erineva rikkumisega.

---

[20] Vt ka isikuandmete kaitse üldmääruse põhjendused 85 ja 75.

[21] Vt ka isikuandmete kaitse üldmääruse põhjendus 86.

[22] Täiendavate üksikasjade kohta vt artikli 29 töörühma suunised trahvide kohaldamise ja määramise kohta: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

II. ARTIKKEL 33 - JÄRELEVALVEASUTUSE TEAVITAMINE

A. Millal teatada

1. Artikli 33 nõuded

29. Isikuandmete kaitse üldmääruse artikli 33 lõikes 1 on sätestatud:

> „Isikuandmetega seotud rikkumise korral teatab vastutav töötleja isikuandmetega seotud rikkumisest artikli 55 kohasele pädevale järelevalveasutusele põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus.“

30. Isikuandmete kaitse üldmääruse põhjenduses 87 on märgitud[23]:

> „Tuleks kontrollida, kas kõiki asjakohaseid tehnilisi kaitsemeetmeid ja korralduslikke meetmeid on rakendatud, et teha viivitamata kindlaks, kas isikuandmetega seotud rikkumine on toimunud, ning teavitada sellest kohe järelevalveasutust ning andmesubjekti. Asjaolu, et teavitamine toimus põhjendamatu viivituseta, tuleks kindlaks teha, arvestades eelkõige isikuandmetega seotud rikkumise laadi, tõsidust ja tagajärgi ning kahjulikku mõju andmesubjektile. Sellise teavitamise järel võib asjasse sekkuda järelevalveasutus, kooskõlas talle käesolevas määruses ette nähtud ülesannete ja volitustega.“

2. Millal saab vastutav töötleja rikkumisest „teada“?

31. Nagu eespool üksikasjalikult kirjeldatud, nõutakse isikuandmete kaitse üldmääruses, et rikkumise korral teatab vastutav töötleja rikkumisest põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist. Siit võib tekkida küsimus, mis hetkest saab öelda, et vastutav töötleja on saanud rikkumisest „teada“. Euroopa Andmekaitsenõukogu leiab, et vastutav töötleja on saanud rikkumisest „teada“, kui ta on piisavalt kindel, et toimunud on turvaintsident, mille tulemusel on isikuandmete turvalisust rikutud.

32. Kuid nagu eespool märgitud, nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja rakendaks kõiki asjakohaseid tehnilisi kaitsemeetmeid ja korralduslikke meetmeid, et teha viivitamata kindlaks, kas isikuandmetega seotud rikkumine on toimunud, ning teavitaks sellest kohe järelevalveasutust ning andmesubjekte. Samuti on määruses kirjas, et asjaolu, et teavitamine toimus põhjendamatu viivituseta, tuleks kindlaks teha, arvestades eelkõige isikuandmetega seotud rikkumise laadi, tõsidust ja tagajärgi ning kahjulikku mõju andmesubjektile[24]. See seab vastutavale töötlejale kohustuse tagada, et ta saab mis tahes rikkumistest „teada“ õigeaegselt, nii et ta saaks astuda asjakohaseid samme.

33. Millal täpselt võib öelda, et vastutav töötleja on konkreetsest rikkumisest „teada“ saanud, sõltub iga rikkumise asjaoludest. Mõnel juhul on kohe võrdlemisi selge, et rikkumine on toime pandud, samas kui teistel juhtudel võib alles mõne aja järel olla võimalik kindlaks teha, et isikuandmete turvalisust on rikutud. Põhirõhk peaks siiski olema intsidendi viivitamatul uurimisel, et teha kindlaks, kas isikuandmeid on tõepoolest rikutud, ning kui see on nii, siis võtta parandusmeetmeid ja rikkumisest vajaduse korral teatada.

> **Näited**

[23] Siinkohal on oluline ka isikuandmete kaitse üldmääruse põhjendus 85.

[24] Vt isikuandmete kaitse üldmääruse põhjendus 87.

1. Krüpteerimata isikuandmetega USB-mälupulga kaotamise korral ei ole sageli võimalik kindlaks teha, kas volitamata isikutel oli andmetele juurdepääs. Aga isegi kui vastutav töötleja ei pruugi olla suuteline kindlaks tegema, kas konfidentsiaalsusega seotud rikkumine on toimunud, tuleb sellisest juhtumist ikkagi teada anda, kuna on võimalik piisava kindlusega väita, et toimunud on kättesaadavusega seotud rikkumine. Vastutav töötleja pidi sellest „teada“ saama, kui mõistis, et USB-mälupulk on kaduma läinud.

2. Kolmas osapool teavitab vastutavat töötlejat, et ta on juhuslikult saanud ühe kliendi isikuandmed, ja esitab tõendid loata avalikustamise kohta. Kuna vastutavale töötlejale on esitatud selged tõendid konfidentsiaalsusega seotud rikkumise kohta, ei ole kahtlustki, et ta on rikkumisest „teada“ saanud.

3. Vastutav töötleja avastab, et on toimunud võimalik sissetung tema võrku. Vastutav töötleja kontrollib oma süsteeme, et teha kindlaks, kas süsteemis talletatud isikuandmete turvalisus on rikutud, ning kinnitab seda. Kuna vastutaval töötlejal on rikkumise kohta selged tõendid, ei ole ka sellisel juhul kahtlust, et ta on rikkumisest „teada“ saanud.

4. Pärast süsteemi häkkimist võtab küberkurjategija vastutava töötlejaga ühendust, et nõuda lunaraha. Sellisel juhul on vastutaval töötlejal pärast seda, kui ta on kontrollinud oma süsteemi, et teha kindlaks kas seda on rünnatud, kindlad tõendid selle kohta, et rikkumine on tõepoolest toimunud, ning ei ole kahtlustki, et vastutav töötleja on saanud sellest teada.

34. Pärast võimaliku rikkumise kohta teavet saamist üksikisikult, meediaettevõttelt või muust allikast või kui vastutav töötleja on ise avastanud turvaintsidendi, võib vastutav töötleja korraldada lühiajalise uurimise, et teha kindlaks, kas rikkumine on tegelikult toimunud või mitte. Uurimise ajal ei saa väita, et vastutav töötleja on rikkumisest „teada“ saanud. Siiski eeldatakse, et esialgse uurimisega alustatakse võimalikult vara ning et tuvastatakse piisava kindlusega, kas rikkumine on toime pandud; seejärel võib korraldada põhjalikuma uurimise.

35. Kui vastutav töötleja on rikkumisest teada saanud, tuleb teavitamisele kuuluvast rikkumisest teada anda põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul. Selle aja jooksul peaks vastutav töötleja hindama ohtu, mida rikkumine võib üksikisikutele avaldada, et teha kindlaks, kas on tekkinud rikkumisest teatamise kohustus ning kas rikkumisega tegelemiseks on vaja võtta meetmeid. Vastutaval töötlejal võib juba olla olemas rikkumisest tuleneva võimaliku ohu esialgne hinnang, mis on tehtud andmekaitsealase mõjuhinnangu [25] raames enne asjaomase töötlemistoimingu tegemist. Andmekaitsealane mõjuhinnang võib aga olla üldisem võrreldes tegeliku rikkumise konkreetsete asjaoludega ja seega tuleb igal juhul teha täiendav hindamine, mille käigus võetakse arvesse konkreetseid asjaolusid. Üksikasjalikum teave ohu hindamise kohta on esitatud IV jaos.

36. Enamikul juhtudel tuleks selliste esialgsete tegevustega alustada kohe pärast esmast hoiatust (st kui vastutav töötleja või volitatud töötleja kahtlustab, et toimunud on turvaintsident, mis võib hõlmata isikuandmeid). Vaid erakorraliste juhtumite puhul võib see kauem aega võtta.

Näide

Üksikisik teavitab vastutavat töötlejat, et on saanud vastutava töötleja nimel e-kirja, mis sisaldab isikuandmeid, mis on seotud sellega, palju isik on vastutava töötleja pakutud teenust (tegelikult) kasutanud, mis viitaks justkui sellele, et vastutava töötleja andmete turvalisust on rikutud. Vastutav töötleja korraldab lühiajalise uurimise, teeb kindlaks, et tema võrku on sisse tungitud, ja leiab tõendeid isikuandmetele loata juurdepääsu kohta. Nüüd arvestatakse, et vastutav töötleja on saanud rikkumisest „teada“, ja sellest tuleb teavitada järelevalveasutust, välja arvatud juhul, kui rikkumine ei

[25] Vt artikli 29 töörühma WP 248 suunised, mis käsitlevad andmekaitsealast mõjuhinnangut: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

kujuta endast tõenäoliselt ohtu üksikisikute õigustele ega vabadustele. Vastutav töötleja peab võtma rikkumisega tegelemiseks sobivad parandusmeetmed.

37. Seega peab vastutav töötleja olema kehtestanud ettevõttesisesed menetlused rikkumiste avastamiseks ja käsitlemiseks. Näiteks võib vastutav töötleja või volitatud töötleja andmetöötluses ebakorrapärasuste avastamiseks kasutada selliseid tehnilisi meetmeid nagu andmevoo- ja logianalüsaatorid, mille abil on võimalik määratleda sündmusi ja hoiatusi mis tahes logiandmeid seostades[26]. On oluline, et rikkumise avastamise korral teavitatakse sellest asjakohaseid kõrgemal tasemel juhte, et rikkumisega saaks tegeleda ja vajaduse korral sellest teatada kooskõlas artikliga 33 ja vajaduse korral artikliga 34. Selliseid meetmeid ja teavitamismehhanisme võib üksikasjalikult kirjeldada vastutava töötleja intsidentidele reageerimise plaanides ja/või intsidentide juhtimise korras. Nende abil saab vastutav töötleja tõhusalt kavandada ja teha kindlaks, kes vastutab organisatsioonis rikkumise lahendamise juhtimise eest ning kuidas või kas suunata selle lahendamine vastavalt vajadusele kõrgemal tasemel juhtkonnale.

38. Vastutav töötleja peaks samuti olema kehtestanud korra seoses volitatud töötlejatega, keda ta kasutab; volitatud töötlejal on omakorda kohustus rikkumise korral teavitada vastutavat töötlejat (vt allpool).

39. Ehkki rikkumise ärahoidmiseks, sellele reageerimiseks ja sellega tegelemiseks sobilike meetmete kehtestamise vastutus lasub vastutavatel töötlejatel ja volitatud töötlejatel, tuleks teatavaid praktilisi samme astuda igal juhul.

    - Teave kõikide turvalisusega seotud juhtumite kohta tuleks suunata vastutavale isikule või isikutele, kellel on ülesanne tegeleda intsidentidega, teha kindlaks rikkumise esinemine ja hinnata ohtu.
    - Rikkumise tulemusel üksikisikutele avalduvat ohtu tuleks seejärel hinnata (tõenäosus, et ohtu ei ole, oht esineb või oht on suur) ja teavitada organisatsiooni asjaomaseid osakondi.
    - Teavitada tuleks järelevalveasutust ning vajaduse korral tuleks teave rikkumise kohta edastada mõjutatud isikutele.
    - Samal ajal peaks vastutav töötleja tegutsema selle nimel, et rikkumise ulatust piirata ja esialgne olukord taastada. Rikkumine tuleks dokumenteerida vastavalt selle toimumisele.

40. Seega peaks olema selge, et vastutaval töötlejal on kohustus tegutseda kõikide esmaste hoiatuste puhul ja teha kindlaks, kas rikkumine on tegelikult toimunud või mitte. Selle lühikese aja jooksul saab asja põgusalt uurida ning vastutav töötleja saab koguda tõendeid ja muid asjakohaseid detaile. Ent kui vastutav töötleja on piisava kindlusega tuvastanud, et rikkumine on toime pandud, ja kui isikuandmete kaitse üldmääruse artikli 33 lõike 1 tingimused on täidetud, peab ta teavitama sellest järelevalveasutust põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul[27]. Kui vastutav töötleja ei tegutse õigeaegselt ja selgub, et rikkumine on toime pandud, võib seda pidada isikuandmete kaitse üldmääruse artikli 33 alusel teatamata jätmiseks.

41. Isikuandmete kaitse üldmääruse artiklis 32 on selgelt sätestatud, et vastutaval töötlejal ja volitatud töötlejal peaksid olema asjakohased tehnilised ja korralduslikud meetmed, et tagada isikuandmete asjakohane turvalisuse tase: võime rikkumine avastada, sellega tegeleda ja sellest õigeaegselt teada anda tuleks pidada nende meetmete oluliseks osaks.

[26] Olgu märgitud, et näiteks andmete salvestamise, muutmise või kustutamise auditeerimist hõlbustavaid logiandmeid võib samuti käsitada vastava töötlemistoimingu algatanud isiku isikuandmetena.

[27] Vt määrus nr 1182/71, millega määratakse kindlaks ajavahemike, kuupäevade ja tähtaegade suhtes kohaldatavad eeskirjad, kättesaadav aadressil http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:31971R1182&from=ET

3. Kaasvastutavad töötlejad

42. Isikuandmete kaitse üldmääruse artiklis 26 käsitletakse kaasvastutavaid töötlejaid ning täpsustatakse, et kaasvastutavad töötlejad määravad oma asjaomase vastutusvaldkonna isikuandmete kaitse üldmääruse täitmisel [28] . See tähendab ka, et määratakse kindlaks, kumb osapool vastutab isikuandmete kaitse üldmääruse artiklite 33 ja 34 kohaste kohustuste täitmise eest. Euroopa Andmekaitsenõukogu soovitab, et lepingupõhised kokkulepped kaasvastutajate vahel sisaldaks sätteid, millega määratakse kindlaks, kumb kaasvastutajatest on juhtiv või vastutav isikuandmete kaitse üldmääruses kehtestatud rikkumisest teatamise kohustuse eest.

4. Volitatud töötleja kohustused

43. Üldine vastutus isikuandmete kaitse eest lasub vastutaval töötlejal, kuid volitatud töötlejal on täita oluline roll, et võimaldada vastutaval töötlejal oma kohustusi täita. Nende hulka kuulub rikkumisest teatamine. Isikuandmete kaitse üldmääruse artikli 28 lõikes 3 on täpsustatud, et volitatud töötleja töötleb andmeid siduva lepingu või muu siduva õigusakti alusel. Artikli 28 lõike 3 punktis f on kirjas, et lepingus või muus õigusaktis sätestatakse, et volitatud töötleja „aitab vastutaval töötlejal täita artiklites 32–36 sätestatud kohustusi, võttes arvesse isikuandmete töötlemise laadi ja volitatud töötlejale kättesaadavat teavet“.

44. Isikuandmete kaitse üldmääruse artikli 33 lõikes 2 on selgelt öeldud, et kui vastutav töötleja kasutab volitatud töötleja teenuseid ning volitatud töötleja saab teada nende isikuandmetega seotud rikkumisest, mida ta vastutava töötleja heaks töötleb, peab ta vastutavat töötlejat teavitama põhjendamatu viivituseta. Olgu märgitud, et volitatud töötleja ei pea enne vastutava töötleja teavitamist kõigepealt hindama rikkumisest tuleneva ohu tõenäosust; selle hinnangu peab andma vastutav töötleja rikkumisest teada saamisel. Volitatud töötleja peab üksnes kindlaks tegema, kas rikkumine on toimunud, ja seejärel teavitama sellest vastutavat töötlejat. Vastutav töötleja kasutab volitatud töötleja teenuseid oma eesmärkide täitmiseks; seega peaks põhimõtteliselt saama öelda, et vastutav töötleja on saanud rikkumisest „teada“, kui volitatud töötleja on teda sellest teavitanud. Volitatud töötleja kohustus vastutavat töötlejat teavitada võimaldab vastutaval töötlejal rikkumisega tegeleda ja teha kindlaks, kas ta peab või ei pea sellest teavitama järelevalveasutust kooskõlas artikli 33 lõikega 1 ning mõjutatud üksikisikuid kooskõlas artikli 34 lõikega 1. Vastutav töötleja võib samuti soovida rikkumist uurida, kuna volitatud töötleja positsiooni tõttu ei pruugi ta teada kõiki teemaga seotud asjaolusid, näiteks kas vastutaval töötlejal on endiselt alles koopia või varukoopia isikuandmetest, mille volitatud töötleja hävitas või kaotas. See asjaolu võib mõjutada otsust, kas vastutav töötleja peab rikkumisest teada andma.

45. Isikuandmete kaitse üldmääruses ei ole kehtestatud kindlat tähtaega, mille jooksul volitatud töötleja peab vastutavat töötlejat hoiatama, välja arvatud juhud, kui seda tuleb teha „põhjendamatu viivituseta“. Seetõttu soovitab Euroopa Andmekaitsenõukogu, et volitatud töötleja teavitab vastutavat töötlejat kohe ning edasine teave rikkumise kohta edastatakse järk-järgult uute asjaolude ilmnemisel. See on oluline, et aidata vastutaval töötlejal täita kohustust teavitada järelevalveasutust 72 tunni jooksul.

46. Nagu eespool selgitatud, tuleb vastutava töötleja ja volitatud töötleja vahelises lepingus täpsustada, kuidas lisaks isikuandmete kaitse üldmääruse teiste sätete nõuetele täidetakse artikli 33 lõikes 2 kehtestatud nõudeid. See võib hõlmata volitatud töötleja suhtes kehtestatud varajase teatamise nõuet, mis omakorda toetab vastutava töötleja kohustust teavitada järelevalveasutust 72 tunni jooksul.

47. Kui volitatud töötleja pakub teenuseid mitmele vastutavale töötlejale, keda sama intsident mõjutab, peab volitatud töötleja teavitama intsidendi üksikasjadest kõiki vastutavaid töötlejaid.

---

[28] Vt ka isikuandmete kaitse üldmääruse põhjendus 79.

48. Volitatud töötleja võib rikkumisest teatada vastutava töötleja nimel, kui vastutav töötleja on volitatud töötlejale andnud asjakohase volituse ja see on vastutava töötleja ja volitatud töötleja vahelistes lepingulises kokkuleppes. Selline teavitamine peab toimuma kooskõlas isikuandmete kaitse üldmääruse artiklitega 33 ja 34. Siiski on oluline märkida, et õiguslik vastutus rikkumisest teatamise eest lasub vastutaval töötlejal.

B. Järelevalveasutuse teavitamine

1. Esitatav teave

49. Kui vastutav töötleja teavitab järelevalveasutust rikkumisest, tuleks isikuandmete kaitse üldmääruse artikli 33 lõike 3 kohaselt teha vähemalt järgmist:

> „a) kirjeldada isikuandmetega seotud rikkumise laadi ning nimetada võimaluse korral asjaomaste andmesubjektide kategooriad ja ligikaudne arv ning isikuandmete asjaomaste kirjete liigid ja ligikaudne arv;
>
> b) teatada andmekaitseametniku või mõne teise täiendavat teavet andva kontaktisiku nimi ja kontaktandmed;
>
> c) kirjeldada isikuandmetega seotud rikkumise võimalikke tagajärgi;
>
> d) kirjeldada vastutava töötleja poolt võetud või võtmiseks kavandatud meetmeid isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.“

50. Isikuandmete kaitse üldmääruses ei ole andmesubjektide kategooriaid ega isikuandmekirjete liike määratletud. Euroopa Andmekaitsenõukogu soovitab siiski, et andmesubjektide kategooriad põhineksid nende üksikisikute kategooriatel, kelle isikuandmeid rikkumine on mõjutanud: olenevalt kasutatud deskriptoritest võivad need olla näiteks lapsed ja teised haavatavad rühmad, puuetega inimesed, töötajad või kliendid. Samamoodi võivad isikuandmekirjete liigid osutada erinevat liiki kirjetele, mida vastutav töötleja võib töödelda, näiteks terviseandmed, haridust käsitlevad dokumendid, sotsiaalhoolekande teave, finantsandmed, pangakontonumbrid, passinumbrid jne.

51. Isikuandmete kaitse üldmääruse põhjenduses 85 on selgitatud, et teatamise üks eesmärkidest on vähendada üksikisikutele tekkivat kahju. Seega, kui andmesubjektide kategooriatest või isikuandmete liikidest nähtub, et rikkumise tulemusel tekib teatav oht (nt identiteedivargus, pettus, rahaline kaotus, ametisaladuse paljastamine), siis on oluline, et teavitamisel märgitakse need kategooriad ära. Sel moel on see seotud nõudega kirjeldada rikkumise võimalikke tagajärgi.

52. Kui täpset teavet (nt mõjutatud andmesubjektide täpset arvu) ei ole võimalik saada, ei tohiks see rikkumisest õigel ajal teatamist takistada. Isikuandmete kaitse üldmäärusega on lubatud esitada mõjutatud üksikisikute ja asjaomaste isikuandmekirjete ligikaudne arv. Täpsete näitajate esitamise asemel peaks tähelepanu keskmes olema rikkumise kahjulik mõju.

53. Seega, kui on selge, et rikkumine on toimunud, kuid selle ulatus ei ole veel teada, on järkjärguline teatamine (vt allpool) kindel viis teatamiskohustuse täitmiseks.

54. Isikuandmete kaitse üldmääruse artikli 33 lõikes 3 on öeldud, et vastutav töötleja esitab teates „vähemalt“ selle teabe, seega saab vastutav töötleja vajadusel esitada täiendavaid üksikasju. Erinevate rikkumise liikide puhul (konfidentsiaalsus, terviklus või kättesaadavus) võib täiendava teabe esitamine olla vajalik, et täielikult selgitada iga juhtumi asjaolusid.

Näide

Järelevalveasutuse teavitamise käigus võib vastutav töötleja pidada kasulikuks nimetada volitatud töötleja, kui viimane on rikkumise peamine põhjus, eriti kui see on viinud intsidendini, mis mõjutab sama volitatud töötlejat kasutavate teiste vastutavate töötlejate isikuandmekirjeid.

55. Igal juhul võib järelevalveasutus nõuda rikkumise uurimise raames täiendavat teavet.

2. Järkjärguline teatamine

56. Olenevalt rikkumise laadist võib vastutava töötleja poolne täiendav uurimine olla vajalik, et teha kindlaks kõik intsidendiga seotud faktid. Isikuandmete kaitse üldmääruse artikli 33 lõikes 4 on seetõttu sätestatud:

„Juhul ja niivõrd, kui teavet ei ole võimalik esitada samal ajal, võib teabe esitada järk-järgult ilma põhjendamatu viivituseta.“

57. See tähendab, et isikuandmete kaitse üldmääruses tunnistatakse, et vastutavatel töötlejatel ei ole alati 72 tunni jooksul pärast rikkumisest teada saamist kogu vajalikku teavet rikkumise kohta, kuna intsidendi kõik üksikasjad ei pruugi kohe alguses kättesaadavad olla. Seega lubatakse teavet edastada järk-järgult. Selline olukord esineb tõenäolisemalt keerukamate rikkumiste puhul, nagu küberjulgeoleku intsidentide teatud liigid, mille puhul võib osutuda vajalikuks läbi viia põhjalik kohtulik menetlus, et määrata täielikult kindlaks rikkumise laad ja ulatus, mil määral isikuandmete turvalisust on rikutud. Sellest tulenevalt tuleb vastutaval töötlejal paljudel juhtudel asja hiljem põhjalikumalt uurida ja lisada hiljem täiendav teave. See on lubatud, kui vastutav töötleja esitab viivituse põhjused kooskõlas isikuandmete kaitse üldmääruse artikli 33 lõikega 1. Euroopa Andmekaitsenõukogu soovitab, et kui vastutav töötleja teavitab järelevalveasutust esimest korda, peaks ta juhul, kui tal ei ole veel kogu vajalikku teavet ja ta kavatseb esitada täiendavad üksikasjad hiljem, sellest järelevalveasutusele teada andma. Järelevalveasutus peaks selle, kuidas ja millal lisateave esitatakse, heaks kiitma. See ei takista vastutaval töötlejal esitamast täiendavat teavet hilisemates etappides, kui ta saab teada täiendavatest rikkumisega seotud üksikasjadest, mis tuleb järelevalveasutusele edastada.

58. Rikkumisest teatamise nõude eesmärk on innustada vastutavaid töötlejaid rikkumise esinemisel kohe tegutsema, piirama selle ulatust ja võimaluse korral taastama rikutud isikuandmed ning vajadusel küsima järelevalveasutuselt nõu. Järelevalveasutuse teavitamine 72 tunni jooksul võimaldab vastutaval töötlejal tagada, et üksikisikute teavitamisega või mitteteavitamisega seotud otsused on õiged.

59. Järelevalveasutuse teavitamise eesmärk ei ole siiski üksnes saada juhiseid selle kohta, kas mõjutatud üksikisikuid teavitada. Mõnel juhul on selge, et rikkumise laadi ja ohu tõsiduse tõttu peab vastutav töötleja teavitama mõjutatud isikuid viivitamata. Näiteks, kui esineb identiteedivarguse vahetu oht või kui isikuandmete eriliigid[29] avalikustatakse veebis, tuleb vastutaval töötlejal tegutseda põhjendamatu viivituseta, et piirata rikkumise ulatust ja teatada sellest asjaomastele üksikisikutele (vt III jagu). Erandkorras võib see toimuda isegi enne järelevalveasutuse teavitamist. Üldiselt võttes aga ei saa järelevalveasutuse teavitamist kasutada õigustusena, millele tuginedes jätta andmesubjektidele rikkumisest teada andmata, kui see on nõutav.

60. Samuti peaks olema selge, et pärast esialgse teate edastamist võib vastutav töötleja saata järelevalveasutusele uut teavet, kui hilisema uurimise käigus leitakse tõendeid selle kohta, et turvaintsident saadi kontrolli alla ja rikkumist tegelikult ei toimunud. Selle teabe võib lisada teabele, mis on järelevalveasutusele juba edastatud, ning intsidenti ei registreerita rikkumisena. Sellisest intsidendist teatamise eest, mille puhul hiljem selgub, et tegemist ei olnud rikkumisega, ei karistata.

[29] Vt isikuandmete kaitse üldmääruse artikkel 9.

Näide

Vastutav töötleja teavitab järelevalveasutust 72 tunni jooksul pärast seda, kui ta on avastanud rikkumise, et ta on kaotanud USB-mälupulga, millel on osade klientide isikuandmete koopia. Hiljem leitakse, et USB-mälupulk oli vastutava töötleja ruumides valesse kohta pandud, ning andmed taastatakse. Vastutav töötleja saadab järelevalveasutusele uut teavet ja taotleb rikkumisteate muutmist.

61. Olgu märgitud, et järkjärguline lähenemisviis teatamisele on juba kehtestatud direktiivis 2002/58/EÜ, määruses 611/2013 ja teiste intsidentide puhul, millest asjaomane isik on ise teada saanud.

3. Hilisem teatamine

62. Isikuandmete kaitse üldmääruse artikli 33 lõikes 1 on selgitatud, et kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus. Sellega ja järkjärgulise teatamise põhimõttega võetakse arvesse, et vastutav töötleja ei pruugi alati suuta selle aja jooksul rikkumisest teatada ning hilisem teatamine võib olla lubatud.

63. Selline olukord võib tekkida näiteks siis, kui vastutav töötleja puutub lühikese aja jooksul kokku mitme sarnase konfidentsiaalsusega seotud rikkumisega, mis mõjutavad paljusid andmesubjekte samal viisil. Vastutav töötleja võib olla saanud rikkumisest teada ning kui ta alustab uurimist enne rikkumisest teavitamist, võib ta avastada sarnaseid rikkumisi, millel on teised põhjused. Olenevalt asjaoludest võib vastutaval töötlejal kuluda rikkumiste ulatuse kindlakstegemiseks aega ning selle asemel, et igast rikkumisest eraldi teatada, koostab vastutav töötleja sisuka teate mitme väga sarnase rikkumise kohta, mille põhjused võivad olla erinevad. Seetõttu võib järelevalveasutuse teavitamine lükkuda edasi kaugemasse ajavahemikku kui 72 tundi pärast seda, kui vastutav töötleja rikkumistest esimest korda teada sai.

64. Rangelt võttes tuleb teatada igast üksikust rikkumisest. Ülekoormuse vältimiseks võib aga vastutav töötleja esitada koondteate, mis kajastab kõiki asjaomaseid rikkumisi, tingimusel et need kõik on samaliigiliste isikuandmete samalaadsed rikkumised, mis toimusid suhteliselt lühikese aja jooksul. Kui toimub mitu rikkumist, mis on seotud eri liiki isikuandmetega, mida rikutakse erineval viisil, tuleks neist teatada tavapärasel viisil ehk teatada igast rikkumisest kooskõlas artikliga 33.

65. Ehkki isikuandmete kaitse üldmäärusega on hilisem teatamine teataval määral lubatud, ei tohiks seda pidada tavapäraseks teguviisiks. Tasub märkida, et koondteate võib esitada ka mitme sarnase rikkumise kohta, mille kohta esitatakse teade 72 tunni jooksul.

C. Piiriülesed rikkumised ja rikkumised kolmandates riikides

1. Piiriülesed rikkumised

66. Kui toimub isikuandmete piiriülene töötlemine[30], võib rikkumine mõjutada andmesubjekte rohkem kui ühes liikmesriigis. Isikuandmete kaitse üldmääruse artikli 33 lõikes 1 on selgelt öeldud, et rikkumise korral teavitab vastutav töötleja isikuandmetega seotud rikkumisest isikuandmete kaitse üldmääruse[31] artikli 55 kohast pädevat järelevalveasutust. Isikuandmete kaitse üldmääruse artikli 55 lõikes 1 on öeldud:

„Järelevalveasutus on oma liikmesriigi territooriumil pädev täitma ülesandeid ja kasutama volitusi, mis on talle kooskõlas käesoleva määrusega antud.“

67. Isikuandmete kaitse üldmääruse artikli 56 lõikes 1 on aga öeldud:

[30] Vt isikuandmete kaitse üldmääruse artikli 4 punkt 23.

[31] Vt ka isikuandmete kaitse üldmääruse põhjendus 122.

„Ilma et see piiraks artikli 55 kohaldamist, on vastutava töötleja või volitatud töötleja peamise või ainsa tegevuskoha järelevalveasutus pädev tegutsema juhtiva järelevalveasutusena kõnealuse vastutava töötleja või volitatud töötleja tehtud piiriülese isikuandmete töötlemise toimingu suhtes kooskõlas artiklis 60 sätestatud menetlusega."

68. Lisaks on isikuandmete kaitse üldmääruse artikli 56 lõikes 6 öeldud:

„Piiriülese isikuandmete töötlemise toimingu puhul on vastutava töötleja või volitatud töötleja ainus partner juhtiv järelevalveasutus."

69. See tähendab, et kui rikkumine toimub andmete piiriülese töötlemise käigus ja sellest tuleb teatada, peab vastutav töötleja teavitama juhtivat järelevalveasutust [32] . Seega peab vastutav töötleja rikkumisele reageerimise plaani koostades hindama, milline järelevalveasutus on juhtiv järelevalveasutus, keda tuleb rikkumisest teavitada[33]. See võimaldab vastutaval töötlejal rikkumisele kohe reageerida ja täita artiklist 33 tulenevaid kohustusi. Peaks olema selge, et piiriülest andmetöötlust hõlmava rikkumise korral tuleb teade saata juhtivale järelevalveasutusele, kes ei asu tingimata samas kohas, kus asuvad mõjutatud andmesubjektid või kus toimus rikkumine. Juhtiva järelevalveasutuse teavitamisel peaks vastutav töötleja vajaduse korral märkima ära, kas rikkumine hõlmab teistes liikmesriikides asuvaid asutusi ning milliste liikmesriikide andmesubjekte rikkumine tõenäoliselt mõjutab. Kui vastutaval töötlejal on kahtlusi, milline asutus on juhtiv järelevalveasutus, tuleks tal teavitada vähemalt selle asukoha järelevalveasutust, kus rikkumine toimus.

2. Rikkumised kolmandates riikides

70. Isikuandmete kaitse üldmääruse artiklis 3 käsitletakse isikuandmete kaitse üldmääruse territoriaalset kohaldamisala, sealhulgas määruse kohaldamist isikuandmete töötlemise suhtes mujal kui liidus asuva vastutava töötleja või volitatud töötleja poolt. Täpsemalt on isikuandmete kaitse üldmääruse artikli 3 lõikes 2 öeldud[34]:

„Käesolevat määrust kohaldatakse liidus asuvate andmesubjektide isikuandmete töötlemise suhtes mujal kui liidus asuva vastutava töötleja või volitatud töötleja poolt, kui andmete töötlemine on seotud

a) liidus asuvatele andmesubjektidele kaupade ja teenuste pakkumisega, olenemata sellest, kas andmesubjekt peab maksma tasu, või

b) nende tegevuse jälgimisega, kui see tegevus toimub liidus."

71. Samuti on asjakohane isikuandmete kaitse üldmääruse artikli 3 lõige 3, kus on öeldud[35]:

„Käesolevat määrust kohaldatakse isikuandmete töötlemise suhtes vastutava töötleja poolt, kelle asukoht ei ole liidus, vaid kohas, kus rahvusvahelise avaliku õiguse kohaselt kohaldatakse mõne liikmesriigi õigust."

72. Kui mujal kui liidus asuva vastutava töötleja suhtes kohaldatakse isikuandmete kaitse üldmääruse artikli 3 lõiget 2 või 3 ning tema ettevõttes toimub rikkumine, kehtib tema suhtes seega endiselt isikuandmete kaitse üldmääruse artiklitest 33 ja 34 tulenev rikkumisest teatamise kohustus.

[32] Vt artikli 29 töörühma „Vastutava töötleja või volitatud töötleja juhtiva järelevalveasutuse kindlaksmääramise suunised", kättesaadavad aadressil http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] Kõikide Euroopa riiklike andmekaitseametite kontaktandmete loetelu on esitatud aadressil https://edpb.europa.eu/about-edpb/about-edpb/members_en

[34] Vt ka isikuandmete kaitse üldmääruse põhjendused 23 ja 24.

[35] Vt ka isikuandmete kaitse üldmääruse põhjendus 25.

Isikuandmete kaitse üldmääruse artiklis 27 on nõutud, et artikli 3 lõike 2 kohaldamisel määrab vastutav töötleja (ja volitatud töötleja) oma esindaja liidus.

73. Kuid pelgalt esindaja kohalolekust liikmesriigis ühtse kontaktpunkti süsteemi kasutamiseks ei piisa[36]. Seepärast tuleb rikkumisest teavitada kõiki järelevalveasutusi, mille liikmesriigis mõjutatud andmesubjektid elavad. Sellise teatamise eest vastutab vastutav töötleja[37].

74. Samamoodi, kui volitatud töötleja suhtes kohaldatakse isikuandmete kaitse üldmääruse artikli 3 lõiget 2, on ta seotud volitatud töötlejate suhtes kehtivate kohustustega, kusjuures siinkohal on eriti oluline isikuandmete kaitse üldmääruse artikli 33 lõikes 2 sätestatud kohustus teavitada rikkumisest vastutavat töötlejat.

D. Tingimused, mille puhul ei ole vaja rikkumisest teatada

75. Isikuandmete kaitse üldmääruse artikli 33 lõikes 1 on selgelt öeldud, et rikkumistest, mis „ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele“, ei ole järelevalveasutust vaja teavitada. Näitena võib tuua olukorra, kus isikuandmed on avalikult kättesaadavad ja selliste andmete avaldamine ei kujuta endast ohtu üksikisikule. See on vastuolus direktiivis 2009/136/EÜ sätestatud rikkumisest teatamise nõuetega, mis kehtivad üldkasutatavate elektrooniliste sideteenuste osutajate suhtes ja mille kohaselt tuleb pädevale asutusele teatada kõikidest vastavatest rikkumistest.

76. Oma arvamuses 03/2014 rikkumisest teatamise kohta [38] selgitas artikli 29 töörühm, et konfidentsiaalsusega seotud rikkumine, kus isikuandmed on krüpteeritud uusima algoritmi alusel, on ikkagi isikuandmetega seotud rikkumine ja sellest tuleb teatada. Kui aga võtme konfidentsiaalsust ei ole rikutud, st turvanõuete rikkumise käigus ei ole võtme turvalisust rikutud ning see on loodud selliselt, et ilma sellele juurdepääsu loata isikud ei saa seda ühegi olemasoleva tehnilise vahendiga uuesti genereerida, on andmed põhimõtteliselt loetamatud. Seega ei avalda rikkumine tõenäoliselt üksikisikutele kahjulikku mõju ja seetõttu ei ole vaja neile sellest teatada[39]. Aga ka krüpteeritud andmete puhul võib andmete kaotsiminek või muutmine tuua andmesubjektide jaoks kaasa negatiivseid tagajärgi, kui vastutaval töötlejal ei ole nõuetekohaseid varukoopiaid. Sellisel juhul oleks andmesubjektide teavitamine nõutav, isegi kui andmete endi suhtes on rakendatud piisavaid krüpteerimismeetmeid.

77. Artikli 29 töörühm selgitas samuti, et olukord oleks sama, kui isikuandmed, nt salasõnad, räsiti ja soolati turvaliselt, räsiväärtus arvutati uusima krüptograafilise võtmega räsifunktsiooni alusel, andmete räsimiseks kasutatud võtme turvalisust ei rikutud ühegi rikkumise käigus ning andmete räsimiseks kasutatud võti loodi viisil, mida ei saa kindlaks teha ühegi olemasoleva tehnilise vahendi abil ükski isik, kellel puuduvad volitused andmetele juurdepääsuks.

78. Sellest tulenevalt, kui isikuandmed on volitamata isikutele põhimõtteliselt loetamatuks muudetud ja kui andmed ise on koopia või neist on tehtud varukoopia, ei pruugi olla vaja järelevalveasutust nõuetekohaselt krüpteeritud isikuandmete konfidentsiaalsusega seotud rikkumisest teavitada. Seda seetõttu, et selline rikkumine ei põhjusta tõenäoliselt ohtu üksikisikute õigustele ja vabadustele. See

---

[36] Vt artikli 29 töörühma „Vastutava töötleja või volitatud töötleja juhtiva järelevalveasutuse kindlaksmääramise suunised“, kättesaadavad aadressil http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] Kooskõlas suunistega 3/2018 isikuandmete kaitse üldmääruse territoriaalse kohaldamisala kohta (artikkel 3), kättesaadavad aadressil https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, leiab Euroopa Andmekaitsenõukogu, et liidus tegutseva esindaja funktsioon ei ole kooskõlas välise andmekaitseametniku rolliga, mistõttu jääb isikuandmetega seotud rikkumise korral järelevalveasutuse teavitamise kohustus kooskõlas isikuandmete kaitse üldmääruse artikli 27 lõikega 5 vastutavale töötlejale. Esindaja võib siiski kaasata teavitamisprotsessi, kui see on kirjalikus volituses sõnaselgelt sätestatud.

[38] Artikli 29 töörühma arvamus 03/2014 rikkumisest teatamise kohta, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[39] Vt ka määruse 611/2013 artikli 4 lõiked 1 ja 2.

tähendab seda, et puudub ka vajadus teavitada asjaomast üksikisikut, kuna suure ohu tõenäosus on väike. Siiski tuleks meeles pidada, et kuigi alguses võib puududa vajadus rikkumisest teatada, sest ohtu üksikisikute õigustele ja vabadustele tõenäoliselt ei ole, võib olukord aja jooksul muutuda ning ohu olemasolu tuleb uuesti hinnata. Näiteks kui hiljem leitakse, et võtme turvalisus on rikutud, või kui krüpteerimistarkvaras leitakse turvaauk, võib rikkumisest teatamine siiski vajalik olla.

79. Lisaks olgu märgitud, et kui krüpteeritud isikuandmed ei ole varundatud ja toimub rikkumine, siis on tegemist kättesaadavusega seotud rikkumisega, mis võib põhjustada ohtu üksikisikutele, ja seega võib teavitamine osutuda vajalikuks. Samamoodi, kui toimub rikkumine, mille käigus lähevad krüpteeritud andmed kaotsi, ning isegi kui isikuandmete varukoopia on olemas, võib ikkagi olla tegemist rikkumisega, millest on vaja teatada, olenevalt sellest, kui palju aega kulub varukoopiast andmete taastamiseks ja kuidas andmete kättesaadavuse puudumine mõjutab üksikisikuid. Nagu isikuandmete kaitse üldmääruse artikli 32 lõike 1 punktis c on öeldud, on turvalisuse oluline tegur „võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral“.

Näide

Vastutava töötleja ja tema personali käsutuses oleva turvaliselt krüpteeritud mobiilseadme kaotsimineku puhul ei ole vaja järelevalveasutust teavitada. Tingimusel, et krüpteerimisvõti on turvaliselt vastutava töötleja käes ja tegemist ei ole isikuandmete ainsa koopiaga, on isikuandmed ründaja jaoks kättesaamatud. See tähendab, et rikkumisest ei tulene ohtu asjaomaste andmesubjektide õigustele ega vabadustele. Kui hiljem selgub, et krüpteerimisvõtme turvalisus on rikutud või et krüpteerimistarkvaras või algoritmis on turvaauk, muutub üksikisikute õigustele ja vabadustele avalduva ohu suurus ja teavitamine võib nüüd osutuda vajalikuks.

80. Isikuandmete kaitse üldmääruse artikli 33 nõuded ei ole aga täidetud, kui vastutav töötleja ei teavita järelevalveasutust olukorras, kus andmed ei ole tegelikult turvaliselt krüpteeritud. Seega peaksid vastutavad töötlejad krüpteerimistarkvara valimisel hoolikalt kaaluma pakutud krüpteerimisteenuse kvaliteeti ja nõuetekohast rakendamist ning mõistma, millise taseme kaitset tegelikult pakutakse ja kas see on piisav arvestades võimalike ohte. Ka vastutavad töötlejad peaksid nende käsutuses oleva krüptoseadme toimimise eripäradega kursis olema. Näiteks võib seade olla krüpteeritud, kui see on välja lülitatud, kuid mitte ooterežiimis. Osadel krüpteerimist kasutavatel seadmetel on nn vaikimisi klahvid, mida iga kasutaja peab krüpteerimiseks muutma. Isegi kui turvaeksperdid võivad krüpteerimist praegu piisavaks pidada, võib see mõne aasta pärast olla vananenud, mistõttu on kaheldav, kas see seade suudab andmeid piisavalt krüpteerida ja pakkuda nõuetekohast kaitset.

III. ARTIKKEL 34 – ANDMESUBJEKTI TEAVITAMINE

A. Üksikisikute teavitamine

81. Teatud juhtudel peab vastutav töötleja lisaks järelevalveasutuse teavitamisele andma rikkumisest teada ka mõjutatud üksikisikutele.

Isikuandmete kaitse üldmääruse artikli 34 lõikes 1 on öeldud:

„Kui isikuandmetega seotud rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele, teavitab vastutav töötleja andmesubjekti põhjendamatu viivituseta isikuandmetega seotud rikkumisest.“

82. Vastutavad töötlejad peaksid meeles pidama, et järelevalveasutuse teavitamine on kohustuslik, välja arvatud juhul, kui rikkumine ei ohusta tõenäoliselt üksikisikute õigusi ja vabadusi. Lisaks sellele tuleb teavitada ka üksikisikuid, kui rikkumine kujutab endast tõenäoliselt suurt ohtu nende õigustele ja vabadustele. Seetõttu on üksikisikutele rikkumisest teatamise lävend kõrgem kui järelevalveasutuste

puhul ning seega ei ole üksikisikuid vaja kõikidest rikkumistest teavitada, et neid mitte tarbetult tüüdata.

83. Isikuandmete kaitse üldmääruses on öeldud, et üksikisikuid tuleb rikkumisest teavitada „põhjendamatu viivituseta“ ehk nii pea kui võimalik. Üksikisikute teavitamise peamine eesmärk on anda konkreetset teavet meetmete kohta, mida nad peaksid enda kaitseks tegema[40]. Nagu eespool märgitud, võib õigeaegne teavitamine olenevalt rikkumise ja võimaliku ohu laadist aidata üksikisikutel end kaitsta rikkumise kahjulike tagajärgede eest.

84. Käesolevate suuniste lisas B on esitatud mittetäielik nimekiri näidetest olukordadest, kui rikkumine võib põhjustada üksikisikutele suurt ohtu, ja sellest tulenevalt olukordadest, kui vastutav töötleja peab mõjutatud isikuid rikkumisest teavitama.

B. Esitatav teave

85. Üksikisikute teavitamise kohta on isikuandmete kaitse üldmääruse artikli 34 lõikes 2 täpsustatud:

> „Andmesubjektile käesoleva artikli lõike 1 kohaselt esitatud teates kirjeldatakse selges ja lihtsas keeles isikuandmetega seotud rikkumise laadi ning esitatakse vähemalt artikli 33 lõike 3 punktides b, c ja d osutatud teave ja meetmed.“

86. Selle sätte kohaselt peaks vastutav töötleja esitama vähemalt järgmise teabe:

- kirjeldus rikkumise laadist;
- andmekaitseametniku või mõne teise kontaktisiku nime ja kontaktandmed;
- kirjeldus rikkumise võimalikest tagajärgedest ja
- vastutava töötleja poolt rikkumise lahendamiseks võetud või võtmiseks kavandatud meetmete kirjeldus, sealhulgas vajaduse korral meetmed rikkumise võimaliku kahjuliku mõju leevendamiseks.

87. Näitena meetmetest, mis on võetud rikkumise lahendamiseks ja võimaliku kahjuliku mõju leevendamiseks, võib vastutav töötleja teatada, et pärast pädevale järelevalveasutusele rikkumisest teatamist on vastutav töötleja saanud nõu, kuidas rikkumisega tegeleda ja selle mõju vähendada. Vastutav töötleja peaks vajadusel andma üksikisikutele ka konkreetseid soovitusi, et nad saaksid end kaitsta rikkumise võimalike kahjulike tagajärgede eest, näiteks määrama uue salasõna, kui juurdepääsumandaadi turvalisust on rikutud. Ka sellisel juhul võib vastutav töötleja valida, millist teavet ta lisaks nõutud teabele edastab.

C. Üksikisikutega kontakteerumine

88. Põhimõtteliselt tuleb mõjutatud andmesubjekte rikkumisest teavitada otse, välja arvatud juhul, kui see nõuab ebaproportsionaalselt suurt jõupingutust. Sellisel juhul tehakse avalik teadaanne või võetakse muu sarnane meede, millega teavitatakse kõiki andmesubjekte võrdselt tulemuslikul viisil (isikuandmete kaitse üldmääruse artikli 34 lõike 3 punkt c).

89. Andmesubjekte tuleks rikkumisest teavitada pühendatud sõnumite kaudu, mida ei tohiks edastada koos muu teabega, näiteks korrapäraste uuendustega, uudiskirjadega või tavasõnumitega. See aitab rikkumisest teavitamise muuta selgeks ja läbipaistvaks.

90. Läbipaistva teabevahetuse näidete hulgas on otseedastus (nt e-post, SMS, otsesõnum), silmapaistvad bännerid või teated veebisaidil, otsepostitus ja silmapaistvad reklaamid trükimeedias. Üksnes pressiteates või äriühingu blogis esitatud teade ei ole tõhus viis, kuidas üksikisikuid rikkumisest teavitada. Euroopa Andmekaitsenõukogu soovitab vastutavatel töötlejatel valida vahendi, mille puhul on tõenäosus, et teave jõuab nõuetekohaselt kõikide mõjutatud üksikisikuteni, võimalikult suur.

[40] Vt ka isikuandmete kaitse üldmääruse põhjendus 86.

Olenevalt olukorrast võib see tähendada, et vastutav töötleja kasutab ühe suhtluskanali asemel mitut suhtluskanalit.

91. Vastutavatel töötlejatel võib tekkida ka vajadus tagada, et teabevahetus on ligipääsetav sobivates alternatiivsetes vormingutes ja asjaomastes keeltes tagamaks, et üksikisikud saavad neile edastatud teabest aru. Näiteks sobib üksikisikute rikkumisest teavitamiseks üldiselt keel, mida kasutatakse vastuvõtjaga tavapärases ärisuhtluses. Kui aga rikkumine mõjutab andmesubjekte, kellega vastutav töötleja ei ole varem suhelnud või kes elavad muus liikmesriigis või kolmandas riigis kui vastutava töötleja asukohariik, võib suhtlemine kohalikus keeles olla vastuvõetav, võttes arvesse selleks vajalikke ressursse. Peamine on aidata andmesubjektidel mõista rikkumise laadi ja samme, mida nad saavad enda kaitseks astuda.

92. Kõige paremini saavad üksikisikute teavitamiseks sobiva suhtluskanali kindlaks teha vastutavad töötlejad, eriti juhul, kui nad suhtlevad klientidega sageli. Siiski on ilmselge, et vastutav töötleja peab olema rikkumise tõttu ohtu sattunud suhtluskanali kasutamisel ettevaatlik, kuna seda võivad kasutada ka vastutava töötleja nime all esinevad ründajad.

93. Samas on isikuandmete kaitse üldmääruse põhjenduses 86 selgitatud:

> „Teade tuleks saata andmesubjektile nii kiiresti kui mõistlikkuse piires võimalik ning tihedas koostöös järelevalveasutusega, pidades kinni tema või muude asjakohaste asutuste nagu näiteks õiguskaitseasutuste suunistest. Näiteks kahju tekkimise otsese ohu leevendamise vajadus eeldaks andmesubjekti kohest teavitamist, samal ajal kui vajadus rakendada asjakohaseid meetmeid isikuandmetega seonduvate rikkumiste jätkumise või samalaadsete isikuandmetega seonduvate rikkumiste ärahoidmiseks võib õigustada hilisemat teavitamist.“

94. Vastutavad töötlejad võivad seetõttu soovida kontakteeruda ja pidada nõu järelevalveasutusega, et küsida nõu mitte ainult andmesubjektidele kooskõlas artikliga 34 rikkumisest teatamise kohta, vaid ka selle kohta, milliseid teateid on kõige asjakohasem üksikisikutele saata ja milline on sobivaim kontakteerumisviis.

95. Sellega on seotud isikuandmete kaitse üldmääruse põhjenduses 88 antud soovitus, et rikkumisest teavitamisel tuleks „arvesse võtta õiguskaitseasutuste õigustatud huve juhtudel, kui varajane avalikustamine võib tarbetult takistada isikuandmetega seotud rikkumise asjaolude uurimist“. See võib tähendada, et teatud olukorras, kui see on õigustatud ja kui õiguskaitseasutused on andnud sellist nõu, võib vastutav töötleja viivitada mõjutatud isikutele rikkumisest teatamisega seni, kuni see ei takista uurimist. Pärast sellist viivitust tuleb andmesubjekte siiski kohe teavitada.

96. Kui vastutav töötleja ei saa üksikisikut rikkumisest teavitada, sest temaga kontakteerumiseks ei ole piisavalt andmeid, peab vastutav töötleja sellisel konkreetsel juhul teavitama üksikisikut nii kiiresti, kui see on mõistlikult võimalik (nt kui üksikisik kasutab oma artiklist 15 tulenevat õigust tutvuda isikuandmetega ning esitab vastutavale töötlejale temaga kontakteerumiseks vajaliku lisateabe).

D. Tingimused, mille puhul ei ole vaja rikkumisest teatada

97. Isikuandmete kaitse üldmääruse artikli 34 lõikes 3 on esitatud kolm tingimust, mille täitmise korral ei ole vaja rikkumisest üksikisikuid teavitada. Need on järgnevad.

    - Vastutav töötleja on enne rikkumist kohaldanud isikuandmete kaitsmiseks nõuetekohaseid tehnilisi ja korralduslikke meetmeid, eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsuõiguseta isikutele loetamatuks. See võib hõlmata näiteks isikuandmete kaitsmist uusima krüpteeringu või tingnimestuse abil.
    - Vastutav töötleja on kohe pärast rikkumist astunud samme tagamaks, et suure ohu teke andmesubjektide õigustele ja vabadustele ei ole enam tõenäoline. Näiteks, olenevalt olukorrast, võis vastutav töötleja suuta isikuandmetele juurde pääsenud isiku kohe kindlaks teha ja võtta tema vastu meetmeid enne, kui ta sai nende andmetega midagi ette võtta. Aga

ka sellisel juhul tuleb analüüsida konfidentsiaalsusega seotud rikkumise võimalikke tagajärgi ja teha seda olenevalt asjaomaste andmete laadist.

- Üksikisikutega kontakteerumine nõuaks ebaproportsionaalseid jõupingutusi[41] näiteks siis, kui nende kontaktandmed on rikkumise tõttu kadunud või neid ei olnud algusest peale teada. Näiteks, statistikabüroo ladu ujutas üle ja isikuandmeid sisaldavaid dokumente talletati ainult paberkujul. Vastutav töötleja peab tegema avaliku teadaande või võtma muu sarnase meetme, millega teavitatakse üksikisikuid võrdselt tõhusal viisil. Ebaproportsionaalse jõupingutuse vältimiseks võib näha ette ka tehnilise korra, mille alusel teha rikkumisega seotud teave nõudlusel kättesaadavaks– sellest võib abi olla rikkumise tõttu mõjutatud üksikisikutel, kellega vastutav töötleja ei saa muul viisil kontakteeruda.

98. Vastutavad töötlejad peaksid kooskõlas vastutuse põhimõttega suutma järelevalveasutusele tõendada, et nad täidavad ühte või mitut nimetatud tingimust[42]. Tuleks meeles pidada, et kuigi alguses võib puududa vajadus rikkumisest teatada, sest ohtu üksikisikute õigustele ja vabadustele ei ole, võib olukord aja jooksul muutuda ning ohu olemasolu tuleb uuesti hinnata.

99. Kui vastutav töötleja otsustab üksikisikuid rikkumisest mitte teavitada, on isikuandmete kaitse üldmääruse artikli 34 lõikes 4 selgitatud, et järelevalveasutus võib seda nõuda, kui ta leiab, et rikkumine kujutab endast üksikisikutele tõenäoliselt suurt ohtu. Järelevalveasutus võib ka otsustada, et isikuandmete kaitse üldmääruse artikli 34 lõike 3 tingimused on täidetud, ja sellisel juhul ei ole vaja üksikisikuid teavitada. Kui järelevalveasutus leiab, et otsus andmesubjekte mitte teavitada ei ole hästi põhjendatud, võib ta kaaluda parandus- ja karistuste kehtestamise volituste kasutamist.

IV. OHU JA SUURE OHU HINDAMINE

A. Oht kui rikkumisest teatamise käivitaja

100. Ehkki isikuandmete kaitse üldmääruses on kehtestatud kohustus rikkumisest teatada, ei kehti see nõue kõikides olukordades.

- Pädeva järelevalveasutuse teavitamine on vajalik, välja arvatud juhul, kui rikkumisest ei tulene tõenäoliselt ohtu üksikisikute õigustele ja vabadustele.
- Üksikisikule teatatakse rikkumisest üksnes siis, kui rikkumisest tuleneb tõenäoliselt suur oht nende õigustele ja vabadustele.

101. See tähendab, et vahetult pärast rikkumisest teada saamist on väga oluline, et vastutav töötleja peaks lisaks intsidendi ulatuse piiramisele püüdma hinnata ka sellest tuleneda võivat ohtu. Selleks on kaks olulist põhjust: esiteks, teades üksikisikule avalduva mõju tõenäosust ja võimalikku tõsidust, on vastutaval töötlejal lihtsam astuda tulemuslikke samme rikkumise ulatuse piiramiseks ja sellega tegelemiseks; teiseks aitab see kindlaks teha, kas järelevalveasutust ja asjaomaseid üksikisikuid on vaja rikkumisest teavitada.

102. Nagu on eespool selgitatud, on rikkumisest teatamine nõutav, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele, ning peamine põhjus andmesubjektide teavitamiseks on see, kui rikkumisest tuleneb tõenäoliselt *suur* oht üksikisikute õigustele ja vabadustele. Selline oht on olemas, kui rikkumisest võib tuleneda füüsiline, materiaalne või mittemateriaalne kahju üksikisikutele, kelle andmeid on rikutud. Selline kahju on näiteks diskrimineerimine, identiteedivargus või -pettus, rahaline kahju, maine kahjustamine. Kui rikkumisega on seotud isikuandmed, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi veendumusi või ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise,

[41] Vt artikli 29 töörühma suunised läbipaistvuse kohta, milles käsitletakse ebaproportsionaalsete jõupingutuste küsimust, kättesaadavad aadressil http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Vt isikuandmete kaitse üldmääruse artikli 5 lõige 2.

seksuaalelu ning süüteoasjades süüdimõistvate kohtuotsuste ja süütegude ning nendega seotud turvameetmete kohta, tuleks sellise kahju esinemist pidada tõenäoliseks[43].

B. Tegurid, mida kaaluda ohu hindamisel

103. Isikuandmete kaitse üldmääruse põhjendustes 75 ja 76 on soovitatud, et ohu hindamisel tuleks kaaluda nii andmesubjektide õigustele ja vabadustele avalduva ohu tõenäosust kui ka tõsidust. Veel on seal öeldud, et ohtu tuleks hinnata objektiivse hindamise põhjal.

104. Olgu märgitud, et hinnates ohtu, mida rikkumine võib inimeste õigustele ja vabadustele põhjustada, keskendutakse muudele asjadele kui andmekaitsealase mõjuhinnangu [44] käigus ohu hindamisel. Andmekaitsealase mõjuhinnangu käigus kaalutakse nii plaanipäraselt toimuva andmetöötluse ohte kui ka rikkumisest tulenevaid ohte. Võimaliku rikkumise analüüsimisel vaadeldakse üldiselt rikkumise esinemise tõenäosust ja kahju, mis andmesubjektile võib sellega kaasneda; teisisõnu hinnatakse hüpoteetilist sündmust. Tegeliku rikkumise puhul on sündmus juba toimunud ja tähelepanu on täielikult suunatud mõjule, mida rikkumisest tulenev oht üksikisikule avaldab.

Näide

Andmekaitsealase mõjuhinnangu järgi on isikuandmete kaitsmiseks mõeldud turvatarkvara kasutamine sobiv meede, et tagada turvalisuse tase, mis vastab ohule, mida andmete töötlemine võiks muidu üksikisikutele kujutada. Kuid kui seejärel avastatakse turvaauk, muudab see tarkvara sobilikkust piirata kaitstavatele isikuandmetele avalduvat ohtu ja seega tuleb käimasoleva andmekaitsealase mõjuhinnangu käigus tarkvara uuesti hinnata. Tarkvara turvaauku kasutatakse hiljem ära ja toimub rikkumine. Vastutav töötleja peaks hindama rikkumise spetsiifilisi asjaolusid, mõjutatud andmeid ning võimalikku mõju üksikisikutele, samuti seda, kui tõenäoline on, et oht materialiseerub.

105. Sellest tulenevalt peaks vastutav töötleja rikkumisest tuleneva ja üksikisikutele avalduva ohu hindamisel arvestama rikkumise spetsiifilisi asjaolusid, sealhulgas võimaliku mõju tõsidust ja selle tõenäosust. Seepärast soovitab Euroopa Andmekaitsenõukogu, et hindamisel tuleks võtta arvesse järgmisi kriteeriume[45]:

- **Rikkumise liik**

106. Toimunud rikkumise liik võib mõjutada üksikisikutele avalduva ohu suurust. Näiteks võib konfidentsiaalsusega seotud rikkumisel, mille käigus on avaldatud terviseandmeid volitamata isikutele, olla üksikisikule teised tagajärjed kui rikkumisel, kui üksikisiku terviseandmed on kaduma läinud ning ei ole enam kättesaadavad.

- **Isikuandmete laad, tundlikkus ja maht**

107. Kahtlemata on ohu hindamisel väga oluline rikutud isikuandmete liik ja tundlikkus. Tavaliselt on nii, et mida tundlikumad andmed, seda suurem on oht kahju tekkimiseks asjaomastele isikutele, kuid tähelepanu tuleks pöörata ka teistele isikuandmetele, mis võivad juba andmesubjekti kohta kättesaadavad olla. Näiteks ei ole tõenäoline, et üksikisiku nime ja aadressi avaldamine tavaolukorras

[43] Vt isikuandmete kaitse üldmääruse põhjendused 75 ja 85.

[44] Vt töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[45] Määruse 611/2013 artikli 3 lõikes 2 on antud juhiseid asjaolude kohta, mida arvestada seoses rikkumistest teatamisega elektroonilise side teenuste sektoris; nendest võib kasu olla ka isikuandmete kaitse üldmääruse alusel toimuval teavitamisel. Vt http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:et:PDF

põhjustaks olulist kahju. Kuid kui lapsendanud vanema nimi ja aadress avaldatakse bioloogilisele vanemale, võivad tagajärjed olla väga tõsised nii lapsendanud vanema kui ka lapse jaoks.

108. Rikkumised, mis on seotud terviseandmete, isikut tõendavate dokumentide või finantsandmetega, näiteks krediitkaartidega, võivad eraldivõetuna tekitada kahju, kuid koos kasutatuna võib neid kasutada identiteedivarguseks. Isikuandmete kombinatsioon on tavaliselt tundlikum kui üksik osa isikuandmetest.

109. Osa isikuandmete liike võivad esialgu näida võrdlemisi tähtsusetud, kuid siiski tuleb hoolikalt analüüsida, mida need andmed võivad asjaomase üksikisiku kohta avaldada. Nimekiri regulaarselt saadetisi saavatest klientidest ei pruugi väga tundlik olla, kuid samad andmed klientide kohta, kes on palunud puhkuse tõttu saadetiste edastamise peatada, võivad osutuda kurjategijatele kasulikuks teabeks.

110. Samamoodi võib väike hulk väga tundlikke isikuandmeid avaldada üksikisikule suurt mõju ning suur hulk detaile võib avaldada asjaomase üksikisiku kohta palju rohkem teavet. Samuti võib rikkumine, mis mõjutab suuri hulki isikuandmeid mis puudutab paljusid andmesubjekte, avaldada mõju vastavalt suurele üksikisikute arvule.

- **Üksikisikute tuvastamise lihtsus**

111. Oluline on analüüsida, kui lihtne on osapoolel, kellel on juurdepääs rikkumisega seotud isikuandmetele, määrata kindlaks konkreetseid üksikisikuid või sobitada üksikisikute tuvastamiseks nende andmed muu teabega. Olenevalt olukorrast võib tuvastamine olla võimalik otseselt rikutud isikuandmete alusel, ilma et üksikisiku identifitseerimiseks oleks vaja teha eraldi uurimistööd, aga isikuandmete sobitamine konkreetse üksikisikuga võib olla ka äärmiselt raske, kuigi teatud tingimustel võib see siiski võimalik olla. Isiku tuvastamine rikutud andmete alusel võib olla võimalik otseselt või kaudselt, kuid see võib sõltuda ka rikkumise konkreetsetest asjaoludest ning asjaomaste isikuandmete üksikasjade avalikust kättesaadavusest. See võib olla asjakohasem konfidentsiaalsusega ja kättesaadavusega seotud rikkumiste puhul.

112. Nagu eespool öeldud, on nõuetekohase krüpteerimistasemega kaitstud isikuandmed volitamata isikutele, kellel puudub krüpteerimisvõti, loetamatud. Lisaks võib rikkumise korral üksikisikute tuvastamise tõenäosust vähendada pseudonümiseerimine (määratletud isikuandmete kaitse üldmääruse artikli 4 punktis 5 kui „isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid“). Pseudonümiseerimist ei saa eraldivõetuna siiski pidada meetodiks, mis muudab andmed loetamatuks.

- **Tagajärgede tõsidus üksikisikute jaoks**

113. Olenevalt rikkumisega seotud isikuandmete laadist, näiteks kui see puudutab eriliiki isikuandmete kategooriad, võib võimalik kahju üksikisikutele olla eriti suur, eelkõige juhul, kui rikkumise tagajärjeks võib olla identiteedivargus või -pettus, füüsiline kahju, psühholoogiline trauma, alandamine või maine kahjustamine. Kui rikkumine puudutab haavatavate üksikisikute isikuandmeid, võivad need isikud sattuda suuremasse ohtu.

114. See, kas vastutav töötleja teab, et isikuandmed on selliste inimeste valduses, kelle kavatsused ei ole teada või on pahatahtlikud, võib määrata võimaliku ohu taseme. Esineda võib konfidentsiaalsusega seotud rikkumine, mille puhul isikuandmed avalikustatakse ekslikult artikli 4 punktis 10 määratletud kolmandale isikule või teisele vastuvõtjale. See võib juhtuda näiteks juhul, kui isikuandmed saadetakse ekslikult organisatsiooni valesse osakonda või sageli kasutatavale tarnijaorganisatsioonile. Vastutav töötleja võib esitada vastuvõtjale taotluse saadud andmed kas tagastada või turvaliselt hävitada. Mõlemal juhul võib vastuvõtjat pidada „usaldusväärseks“, võttes arvesse, et vastutaval töötlejal on temaga püsiv suhe ja et vastutav töötleja võib olla teadlik tema

toimingutest, varasemast tegevusest ja muudest asjaomastest üksikasjadest. Teisisõnu võib vastutav töötleja teatud kindlusega põhjendatult eeldada, et vastuvõtja ei loe ega kasuta talle ekslikult saadetud andmeid ning täidab juhiseid andmete tagasisaatmise kohta. Isegi kui andmetele on saadud juurdepääs, võib vastutav töötleja ikkagi eeldada, et vastuvõtja ei võta andmetega midagi ette ning tagastab need kohe vastutavale töötlejale ning teeb andmete taastamiseks koostööd. Sellistel juhtudel võib vastutav töötleja seda rikkumisjärgses ohuhinnangus arvesse võtta – asjaolu, et andmete vastuvõtja on usaldusväärne võib vähendada rikkumise tagajärgede tõsidust, kuid see ei tähenda, et rikkumist ei toimunud. Siiski võib see omakorda kõrvaldada üksikisikutele avalduva ohu tõenäosuse, mistõttu ei ole vaja järelevalveasutust või mõjutatud üksikisikuid rikkumisest teavitada. See aga sõltub taas iga konkreetse juhtumi asjaoludest. Sellele vaatamata peab vastutav töötleja ikkagi säilitama teabe rikkumise kohta kui osa oma üldisest kohustusest rikkumised registreerida (vt allpool V jagu).

115. Samuti tuleks arvesse võtta, kas üksikisikutele tekkivad tagajärjed on püsivad, sest kui mõju on pikaajaline, võib seda käsitada suuremana.

- **Üksikisikute eripära**

116. Rikkumine võib mõjutada laste või teiste haavatavate üksikisikute isikuandmeid ja seada nad seetõttu suuremasse ohtu. Üksikisikute puhul võivad esineda ka muud tegurid, mis võivad mõjutada seda, mil määral rikkumine neile mõju avaldab.

- **Vastutava töötleja eripära**

117. Vastutava töötleja roll ja tema tegevuse laad võivad mõjutada seda, kui suur on oht, et rikkumine avaldab üksikisikutele mõju. Näiteks, meditsiiniasutused töötlevad eriliiki isikuandmeid , mis tähendab, et rikkumise puhul ähvardab üksikisikuid suurem oht, kui võrrelda ajalehe meililisti andmetega.

- **Mõjutatud üksikisikute arv**

118. Rikkumine võib mõjutada kas ainult ühte või mõnda üksikisikut või ka mitut tuhandet inimest kui mitte veel rohkemgi. Üldiselt võib tõdeda, et mida suurem on mõjutatud üksikisikute arv, seda suuremat mõju võib rikkumine avaldada. Siiski võib rikkumine tõsiselt mõjutada ka isegi ühte üksikisikut, olenevalt isikuandmete laadist ning kontekstist, kus selle turvalisust rikuti. Ka sellisel juhul on oluline analüüsida kahjuliku mõju tõenäosust ja tõsidust puudutatud isikutele.

- **Üldised tegurid**

119. Seetõttu peab vastutav töötleja rikkumisest tulenevat tõenäolist ohtu hinnates arvesse võtma nii seda, kui tõsine on mõju, mida rikkumine võib üksikisikute õigustele ja vabadustele avaldada, kui ka seda, milline on selle avaldumise tõenäosus. On selge, et kui rikkumise tagajärjed on tõsisemad, on oht suurem ja samamoodi on oht suurem ka juhul, kui tagajärgede esinemise tõenäosus on suurem. Kahtluse korral peaks vastutav töötleja olema pigem ettevaatlik ja rikkumisest teatama. Lisas B esitatakse mitmeid kasulikke näiteid erinevat liiki rikkumiste kohta, millega kaasneb üksikisikutele oht või suur oht.

120. Euroopa Liidu Küberturvalisuse Amet (ENISA) on koostanud soovitused rikkumise tõsiduse hindamise metoodika kohta – kasulik materjal vastutavatele ja volitatud töötlejatele oma rikkumisele reageerimiseplaani[46] koostamisel.

[46] ENISA, Soovitused isikuandmetega seotud rikkumise tõsiduse hindamise metoodika valikul, https://www.enisa.europa.eu/publications/dbn-severity-

V. VASTUTUS JA DOKUMENTEERIMINE

A. Rikkumiste dokumenteerimine

121. Sõltumata sellest, kas rikkumisest tuleb järelevalveasutust teavitada, peab vastutav töötleja kõik rikkumised dokumenteerima, nagu isikuandmete kaitse üldmääruse artikli 33 lõikes 5 on selgitatud:

> „Vastutav töötleja dokumenteerib kõik isikuandmetega seotud rikkumised, sealhulgas isikuandmetega seotud rikkumise asjaolud, selle mõju ja võetud parandusmeetmed. Dokumendid võimaldavad järelevalveasutusel kontrollida käesolevas artiklis sätestatud nõuete täitmist.“

122. See on seotud isikuandmete kaitse üldmääruse artikli 5 lõikes 2 sätestatud vastutuse põhimõttega. Nii teavitamisele mittekuuluvate kui ka teavitamisele kuuluvate rikkumiste registreerimise eesmärk on samuti seotud vastutava töötleja isikuandmete kaitse üldmääruse artiklist 24 tulenevate kohustustega ning järelevalveasutus võib asjaomaseid kandeid nõuda näha. Seetõttu julgustatakse vastutavaid töötlejaid looma asutusesisest rikkumiste registrit hoolimata sellest, kas neil on rikkumisest teatamise kohustus või mitte[47].

123. Ehkki seda, millist meetodit ja struktuuri rikkumiste dokumenteerimisel kasutada, otsustab vastutav töötleja, tuleb teatavad põhiandmed juhtumi kohta alati registreerida. Nagu on nõutud isikuandmete kaitse üldmääruse artikli 33 lõikes 5, peab vastutav töötleja dokumenteerima rikkumisega seotud üksikasjad, mis peaksid hõlmama rikkumise põhjuseid, toimunu kirjeldust ja mõjutatud isikuandmeid. Samuti peaksid need hõlmama rikkumise mõju ja tagajärgi ning vastutava töötleja võetud parandusmeetmeid.

124. Isikuandmete kaitse üldmääruses ei ole täpsustatud selliste dokumentide säilitamise ajavahemikku. Kui sellised dokumendid sisaldavad isikuandmeid, on vastutaval töötlejal kohustus määrata vastavalt isikuandmete töötlemise põhimõtetele[48] kindlaks sobiv dokumentide säilitamise ajavahemik ja tagada, et töötlemine on seaduslik[49]. Vastutaval töötlejal on isikuandmete kaitse üldmääruse artikli 33 lõikest 5 tulenev kohustus dokumentatsioon säilitada, kuna järelevalveasutus võib nõuda tõendite esitamist kõnealuses artiklis sätestatud nõuete või üldisemalt vastutuse põhimõtte täitmise kohta. Selge on see, et kui dokumendid ise isikuandmeid ei sisalda, ei kohaldata ka isikuandmete kaitse üldmääruse säilitamise piirangu põhimõtet[50].

125. Lisaks nendele üksikasjadele soovitab Euroopa Andmekaitsenõukogu, et vastutav töötleja dokumenteeriks ka rikkumisele reageerimiseks tehtud otsuste põhjendused. Eelkõige tuleks asjaomase otsuse põhjendused dokumenteerida juhul, kui rikkumisest ei teatata. Seejuures tuleks esitada ka põhjused, mille alusel vastutav töötleja leiab, et rikkumisest ei tulene tõenäoliselt ohtu üksikisikute õigustele ja vabadustele[51]. Alternatiivina, kui vastutav töötleja leiab, et isikuandmete kaitse üldmääruse artikli 34 lõike 3 mis tahes tingimus on täidetud, peaks ta olema suuteline esitama selle kinnituseks piisavaid tõendeid.

---

[47] Vastutav töötleja võib otsustada dokumenteerida rikkumised sikuandmete töötlemise toimingute registreerimise raames, mida tehakse vastavalt isikuandmete kaitse üldmääruse artiklile 30. Eraldi registrit ei ole vaja, kui rikkumisega seotud teave on selgelt tuvastatav ja taotluse korral saab teha registrist rikkumisega seotud andmete väljavõtte.

[48] Vt isikuandmete kaitse üldmääruse artikkel 5.

[49] Vt isikuandmete kaitse üldmääruse artikkel 6 ja ka artikkel 9.

[50] Vt isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt e.

[51] Vt isikuandmete kaitse üldmääruse põhjendus 85.

126. Kui vastutav töötleja teavitab järelevalveasutust rikkumisest, kuid teatamine viibib, peab vastutav töötleja olema suuteline esitama selle põhjused; viivitamisega seotud dokumentide abil võib olla võimalik näidata, et teatamise viibimine on põhjendatud ega ole ülemäärane.

127. Kui vastutav töötleja teatab rikkumisest mõjutatud üksikisikutele, peaks ta seda tegema läbipaistval viisil ning esitama asjakohast teavet tulemuslikult ja õigeaegselt. Edastatud teabe kohta tõendite säilitamine võiks aidata vastutaval töötlejal näidata, et ta tegutseb vastutustundlikult ja täidab nõudeid.

128. Isikuandmete kaitse üldmääruse artiklite 33 ja 34 nõuete paremaks täitmiseks oleks hea, kui nii vastutaval kui ka volitatud töötlejal oleks dokumenteeritud teatamisprotsess, millega on kehtestatud kord, mida järgida pärast rikkumise avastamist, sealhulgas juhised selle kohta, kuidas intsidendi ulatust piirata, seda ohjata ja andmed taastada ning kuidas ohtu hinnata ja rikkumisest teatada. Isikuandmete kaitse üldmääruse järgimise tõendamiseks võib samuti olla kasulik näidata, et töötajaid on teavitatud selliste protsesside ja mehhanismide olemasolust ning et nad teavad, kuidas rikkumise korral toimida.

129. Olgu märgitud, et kui rikkumine jäetakse nõuetekohaselt dokumenteerimata, võib järelevalveasutus kasutada oma isikuandmete kaitse üldmääruse artiklist 58 tulenevaid volitusi või määrata kooskõlas isikuandmete kaitse üldmääruse artikliga 83 haldustrahvi.

B. Andmekaitseametniku roll

130. Vastutav töötleja või volitatud töötleja võib määrata andmekaitseametniku,[52] nagu seda nõutakse isikuandmete kaitse üldmääruse artiklis 37, või vabatahtlikult head tava järgides. Isikuandmete kaitse üldmääruse artiklis 39 on andmekaitseametnikule kehtestatud mitu kohustuslikku ülesannet, kuid vastutaval töötlejal ei ole keelatud anda talle vajaduse korral täiendavaid ülesandeid.

131. Rikkumisest teatamise puhul on eriti oluline, et andmekaitseametniku kohustuslike ülesannete hulgas oleks muude kohustuste seas vastutavale töötlejale ja volitatud töötlejale andmekaitsealase nõu ja teabe andmine, isikuandmete kaitse üldmääruse järgimise kontrollimine ning nõustamine seoses andmekaitsealase mõjuhinnanguga. Andmekaitseametnik peab tegema järelevalveasutusega koostööd ning tegutsema järelevalveasutuse ja andmesubjektide jaoks kontaktisikuna. Samuti tuleb märkida, et järelevalveasutusele rikkumisest teatamisel peab vastutav töötleja isikuandmete kaitse üldmääruse artiklil 33 lõike 3 punkti b kohaselt edastama oma andmekaitseametniku või muu kontaktisiku nime ja kontaktandmed.

132. Seoses rikkumiste dokumenteerimisega võib vastutav töötleja või volitatud töötleja soovida küsida andmekaitseametniku arvamust dokumentatsiooni struktuuri, loomise ja haldamise kohta. Andmekaitseametnikule võidakse lisaülesandeks anda asjaomaste dokumentide haldamine.

133. Need asjaolud tähendavad, et andmekaitseametnikul peaks olema otsustav roll nii rikkumiste ennetamisel ja nendeks valmistumisel, nõustades ja kontrollides vastavust nõuetele , aga ka rikkumise ajal (st järelevalveasutuse teavitamisel) ja sellele järgneva uurimise ajal, mida korraldab järelevalveasutus. Seda arvestades soovitab Euroopa Andmekaitsenõukogu, et andmekaitseametnikku teavitataks rikkumisest kohe ja et ta kaasataks rikkumise ohjamise ja sellest teatamise protsessi kõikidesse etappidesse.

VI. TEISTEST ÕIGUSAKTIDEST TULENEVAD TEATAMISKOHUSTUSED

134. Lisaks isikuandmete kaitse üldmääruse alusel toimuvale teatamisele ja teabe edastamisele ning üldmäärusest sõltumatult peaksid vastutavad töötlejad olema ka teadlikud turvaintsidentidest

[52] Vt töörühma suunised andmekaitseametnike kohta: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

teatamise nõuetest, mis tulenevad teistest õigusaktidest ja mida võidakse nende suhtes kohaldada, ning sellest, kas seetõttu tuleb neil isikuandmetega seotud rikkumisest teavitada samal ajal ka järelevalveasutust. Sellised nõuded võivad liikmesriigiti erineda; rikkumisest teatamise nõudeid ja nende seost isikuandmete kaitse üldmäärusega on käsitletud näiteks järgmistes õigusaktides:

- *Määrus (EL) 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDASe määrus)*[53].

135. eIDASe määruse artikli 19 lõikes 2 on nõutud, et usaldusteenuse osutajad teavitavad järelevalveasutust igast turvarikkumisest või tervikluse kaost, millel on märkimisväärne mõju osutatavale usaldusteenusele või selles sisalduvatele isikuandmetele. Kui see on kohaldatav – st kui selline rikkumine või kadu on samas ka isikuandmetega seotud rikkumine isikuandmete kaitse üldmääruse alusel, peaks usaldusteenuse osutaja teavitama ka järelevalveasutust.

- *Direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse direktiiv)*[54].

136. Küberturvalisuse direktiivi artiklites 14 ja 16 on nõutud, et oluliste teenuste operaatorid ja digitaalse teenuste osutajad teataksid turvaintsidentidest oma pädevatele asutustele. Nagu küberturvalisuse direktiivi põhjenduses 63[55] on tunnustatud, võib intsidendi tagajärjeks sageli olla isikuandmete kaitse rikkumine. Ehkki küberturvalisuse direktiivis on nõutud, et pädevad asutused ja järelevalveasutused teeksid koostööd ja vahetaksid asjaomast teavet, tuleb asjaomastel operaatoritel ja/või teenuste osutajatel olukorras, kus sellised intsidendid on ka isikuandmete kaitse üldmääruse kohased isikuandmetega seotud rikkumised või võivad nendeks muutuda, teavitada järelevalveasutust eraldi küberturvalisuse direktiivis kehtestatud intsidendist teatamise nõudest.

Näide

Pilveteenuse pakkujal, kes edastab küberturvalisuse direktiivi kohase rikkumise teate, võib olla kohustus teavitada ka vastutavat töötlejat, kui tegemist on isikuandmetega seotud rikkumisega. Sarnaselt võib juhtuda, et usaldusteenuse osutaja, kes edastab teate eIDASe määruse alusel, peab rikkumise esinemise korral teavitama ka asjaomast andmekaitseasutust.

- *Direktiiv 2009/136/EÜ (kodanike õiguste direktiiv) ja määrus 611/2013 (rikkumisest teatamise määrus).*

137. Üldkasutatavate elektroonilise side teenuste osutajad direktiivi 2002/58/EÜ[56] tähenduses peavad rikkumisest teavitama pädevaid riiklikke asutusi.

138. Vastutavad töötlejad peaksid olema teadlikud ka võimalikest täiendavatest õiguslikest, meditsiinilistest või erialastest teatamiskohustustest, mida kohaldatakse mõne muu korra alusel.

---

[53] Vt http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.EST

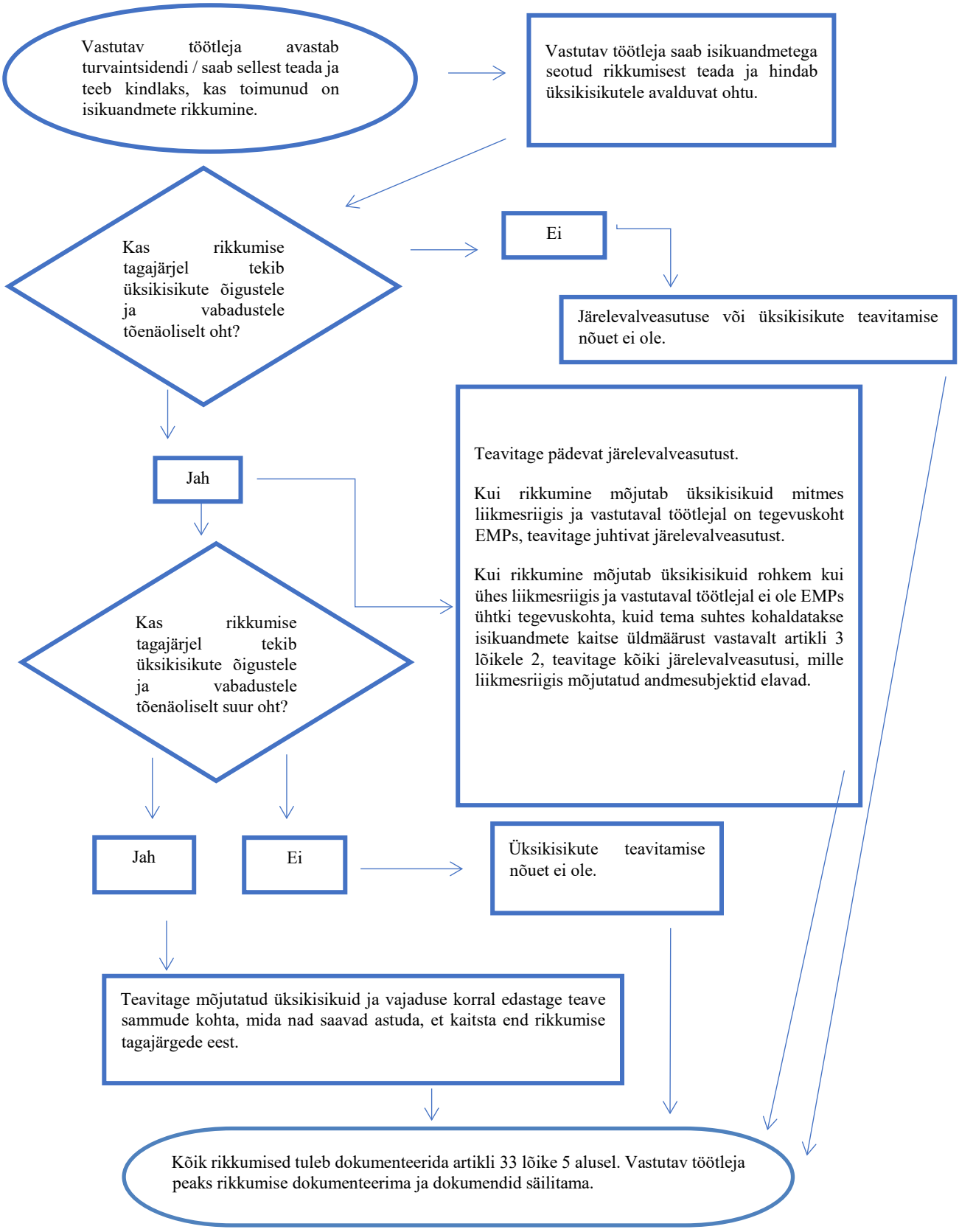
[54] Vt http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.EST

[55] Põhjendus 63: „Sageli on intsidendi tagajärjeks isikuandmete turvalisuse rikkumine. Sellises olukorras peaksid pädevad asutused ja andmekaitseasutused omavahel koostööd tegema ja vahetama teavet kõigis asjaomastes küsimustes, et tulla toime intsidendi tagajärjel toimunud isikuandmetega seotud rikkumisega."

[56] 10. jaanuaril 2017 esitas Euroopa Komisjon ettepaneku privaatsust ja elektroonilist sidet käsitleva määruse kohta, mis asendab direktiivi 2009/136/EÜ ja millest jäetakse välja rikkumisest teatamise nõuded. Kuid kuni ettepanek Euroopa Parlamendis heaks kiidetakse, kehtib rikkumisest teatamise nõue edasi, vt https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. LISA

A. Rikkumisest teatamise nõudeid puudutav vooskeem



B. Näited isikuandmetega seotud rikkumise ja teavitamiskohustuse kohta

Järgmine mitteammendav loetelu näidetest aitab vastutavatel töötlejatel teha kindlaks, kas neil on erinevate isikuandmetega seotud rikkumiste stsenaariumide korral vajadus teavitada. Nende näidete varal saab eristada ka ohtu ja suurt ohtu üksikisikute õigustele ja vabadustele.

Näide	Kas teavitada järelevalveasutust	Kas teavitada andmesubjekti	Märkused/soovitused
i Vastutav töötleja salvestas krüpteeritud isikuandmete arhiivi varukoopia USB-pulgale. USB-pulk varastati sissemurdmise ajal.	Ei	Ei	Seni, kuni andmed on krüpteeritud uusima algoritmi alusel, andmete varukoopiad on olemas ja unikaalse võtme turvalisust ei ole rikutud ning andmeid saab mõistliku aja jooksul taastada, ei pruugi tegemist olla rikkumisega, millest on vaja teatada. Aga kui andmete turvalisust hiljem siiski rikutakse, on teavitamine vajalik.
ii Vastutav töötleja osutab internetipõhist teenust. Selle teenuse vastu suunatud küberrünnaku tõttu lekivad üksikisikute isikuandmed. Vastutava töötleja kliendid on ühes liikmesriigis.	Jah, teavitage järelevalveasutust, kui on tõenäoline, et üksikisikute jaoks tekivad tagajärjed.	Jah, teavitage üksikisikuid olenevalt mõjutatud isikuandmete laadist ja kui tõenäolised tagajärjed üksikisikutele on tõsised.	
iii Põgus mõneminutiline elektrikatkestus vastutava töötleja kõnekeskuses mis tähendab, et kliendid ei saa vastutavale töötlejale helistada ja pääseda juurde oma andmetele.	Ei	Ei	Sellest rikkumisest ei pea teatama, kuid see on intsident, mida tuleb artikli 33 lõike 5 kohaselt dokumenteerida. Vastutav töötleja peaks asjaomaseid andmeid säilitama.

iv	Vastutava töötleja vastu toimub lunavara rünnak, mille tagajärjel kõik andmed krüpteeritakse. Varukoopiad ei ole kättesaadavad ja andmeid ei saa taastada. Uurimise käigus selgub, et lunavara ainus ülesanne oli andmed krüpteerida ja süsteemis muud pahavara ei olnud.	Jah, teavitage järelevalveasutust, kui üksikisikutele tekivad tõenäoliselt tagajärjed, kuna tegemist on kättesaadavuse kaoga.	Jah, teavitage üksikisikuid, olenevalt mõjutatud isikuandmete laadist ja andmete kättesaadavuse puudumise võimalikust mõjust ning muudest võimalikest tagajärgedest.	Kui varukoopia on kättesaadav ja andmed saab taastada õigeaegselt, ei tule sellest järelevalveasutust ja üksikisikuid teavitada, kuna kättesaadavuse ja konfidentsiaalsuse kadu oli ajutine. Kui aga järelevalveasutus saab intsidendist teada muude kanalite kaudu, võib ta kaaluda uurimise läbiviimist, et hinnata artikli 32 turvanõuete järgimist laiemalt.

v	Üksikisik helistab panga kõnekeskusesse ja teatab andmetega seotud rikkumisest. Üksikisik on saanud teise isiku igakuise pangakonto väljavõtte. Vastutav töötleja korraldab lühikese uurimise (st viib selle lõpule 24 tunni jooksul) ja teeb piisava kindlusega selgeks, et toimunud on isikuandmetega seotud rikkumine ja kas tegemist võib olla süsteemse veaga, mis võib tähendada, et mõjutatud on või võivad olla ka teised üksikisikud.	Jah.	Teavitatakse vaid mõjutatud üksikisikuid, kui oht on suur ja on selge, et rikkumine teisi ei mõjutanud.	Kui pärast uurimist selgub, et rikkumine mõjutab rohkemaid üksikisikuid, tuleb järelevalveasutusele edastada täiendavat teavet ja vastutav töötleja astub täiendavaid samme teiste üksikisikute teavitamiseks, kui nende suhtes esineb suur oht.

vi	Vastutav töötleja peab internetipõhist kauplemisplatvormi ja tal on kliente mitmes liikmesriigis. Kauplemisplatvormi vastu toimub küberrünnak ning ründaja avaldab veebis kasutajanimed, salasõnad ja varasemate ostude nimekirjad.	Jah, teavitage juhtivat järelevalveasutust, kui tegemist on piiriülese andmetöötlusega.	Jah, sest sellest võib tuleneda suur oht.	Vastutav töötleja peaks tegutsema, nt tegema mõjutatud kontode salasõnade sundlähtestamise, ning astuma ka muid samme ohu vähendamiseks. Vastutav töötleja peaks kaaluma ka kõiki teisi teatamiskohustusi, nt digitaalse teenuse osutajana küberturvalisuse direktiivi alusel.
vii	Veebimajutust pakkuv ettevõte, kes tegutseb andmete töötlejana, leiab vea koodis, mis kontrollib kasutajalubade andmist. Vea mõjul on kõikidel kasutajatel võimalik pääseda juurde teiste kasutajate kontode üksikasjadele.	Andmete töötlejana peab veebimajutaja viivitamata teavitama mõjutatud kliente (vastutavaid töötlejaid). Oletades, et veebimajutaja on korraldanud ettevõttes uurimise, peaksid mõjutatud vastutavad töötlejad olema piisavalt kindlad selles, kas rikkumine neid puudutab, ja seetõttu loetakse tõenäoliseks, et nad „said sellest teada“, kui veebimajutaja (volitatud töötleja) neid teavitas. Vastutav töötleja peab seejärel teavitama järelevalveasutust.	Kui üksikisikute suhtes suurt ohtu tõenäoliselt ei esine, ei pea neid teavitama.	Veebimajutaja (volitatud töötleja) peab kaaluma kõiki teisi teatamiskohustusi (nt digitaalse teenuse osutajana küberturvalisuse direktiivi alusel). Kui puuduvad tõendid selle kohta, et turvanõrkust kasutatakse ära vastutavate töötlejate poolt, ei pruugi olla vaja rikkumisest teatada, kuid tõenäoliselt tuleb see dokumenteerida või käsitada seda artikli 32 nõuete täitmata jätmisena.
viii	Küberrünnaku tõttu ei ole haiguslood haiglas 30 tunni jooksul kättesaadavad.	Jah, haiglal on kohustus teatada, kuna võib esineda suur oht patsientide heaolule ja privaatsusele.	Jah, teavitage mõjutatud üksikisikuid.	
ix	Suure hulga üliõpilaste isikuandmed saadeti ekslikult valesse meililisti, millel on üle 1000 saaja.	Jah, teavitage järelevalveasutust.	Jah, teavitage üksikisikuid olenevalt asjaomaste isikuandmete ulatusest ja liigist ning võimalike tagajärgede tõsidusest.	

x	Otseturunduse meil edastatakse real „adressaat:“ või „koopia:“ nimetatud saajatele, võimaldades seega igal saajal näha teiste saajate meiliaadresse.	Jah, järelevalveasutuse teavitamine võib olla kohustuslik, kui rikkumine mõjutab paljusid üksikisikuid, kui avaldatud on tundlikke andmeid (nt psühhoterapeudi meililist) või kui teised tegurid põhjustavad suurt ohtu (nt meilis on märgitud algsed salasõnad).	Jah, teavitage üksikisikuid olenevalt asjaomaste isikuandmete ulatusest ja liigist ning võimalike tagajärgede tõsidusest.	Teatamine ei pruugi olla vajalik, kui tundlikke andmeid ei avaldatud ja kui avaldati vaid üksikud meiliaadressid.