ARTIKLI 29 ALUSEL ASUTATUD ANDMETEKAITSE TÖÖRÜHM

18/ET

WP250rev.01

Suunised, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel

Vastu võetud 3. oktoobril 2017

Viimati muudetud ja muudatused vastu võetud 6. veebruaril 2018

Töörühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Töörühm on Euroopa sõltumatu nõuandeorgan andmekaitse ja eraelu puutumatuse küsimustes. Töörühma ülesanded on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaaditeenused tagab Euroopa Komisjoni õigusküsimuste peadirektoraadi direktoraat C (põhiõigused ja liidu kodakondsus), B-1049 Brüssel, Belgia, kabinet nr MO-59 02/013.

Veebisait: https://ec.europa.eu/info/law/law-topic/data-protection_et

TÖÖRÜHM ÜKSIKISIKUTE KAITSEKS SEOSES ISIKUANDMETE TÖÖTLEMISEGA,

mis on asutatud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiviga 95/46/EÜ,

võttes arvesse nimetatud direktiivi artikleid 29 ja 30,

võttes arvesse oma töökorda,

ON VASTU VÕTNUD KÄESOLEVAD SUUNISED:

SISUKORD

SISSEJUHATUS

Isikuandmete kaitse üldmäärusega (GDPR) kehtestatakse nõue teavitada pädevat riiklikku järelevalveasutust[1] (või piiriülese rikkumise korral juhtivat järelevalveasutust) isikuandmetega seotud rikkumisest (edaspidi „rikkumine“) ja teatavatel juhtudel teavitada rikkumisest üksikisikuid, kelle isikuandmeid on rikkumine mõjutanud.

Rikkumisest teatamise kohustus kehtib praegu teatud asutuste, näiteks üldkasutatavate elektrooniliste sideteenuste osutajate suhtes (nagu täpsustatud direktiivis 2009/136/EÜ ja määruses (EL) nr 611/2013)[2]. Leidub ka ELi liikmesriike, kus juba on kehtestatud siseriiklik rikkumisest teavitamise kohustus. See võib hõlmata kohustust teavitada rikkumisest, millega on seotud mitmed vastutavate töötlejate kategooriad lisaks üldkasutatavate elektrooniliste sideteenuste osutajatele (näiteks Saksamaal ja Itaalias), või kohustust teavitada kõikidest isikuandmetega seotud rikkumistest (näiteks Hollandis). Mõnel teisel liikmesriigil on olemas asjaomased tegevusjuhised (näiteks Iirimaa[3]). Ehkki mitmed ELi andmekaitseasutused julgustavad vastutavaid töötlejaid rikkumistest teavitama, ei sisalda andmekaitsedirektiiv 95/46/EÜ,[4] mille asendab isikuandmete kaitse üldmäärus, konkreetset kohustust rikkumisest teavitada ning seega on selline nõue paljudele organisatsioonidele uus. Isikuandmete kaitse üldmäärusega kehtestatakse nüüd kõikide vastutavate töötlejate suhtes teavitamise kohustus, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele[5]. Volitatud töötlejatel on samuti täita oluline roll ja nad peavad teavitama vastutavat töötlejat kõikidest rikkumistest[6].

Artikli 29 töörühm leiab, et uuel 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 rikkumisest asjaomastele üksikisikutele teada anda[7]. Üksikisikute teavitamine võimaldab vastutaval töötlejal edastada teavet rikkumise tulemusel tekkinud ohtude ja sammude kohta, mida need üksikisikud saavad astuda, et ennast kaitsta võimalike tagajärgede eest. Iga rikkumise lahendamise kava eesmärk peaks olema kaitsta üksikisikuid ja nende isikuandmeid. Sellest tulenevalt tuleks rikkumisest teavitamist näha kui vahendit, millega tõhustada isikuandmete kaitsega seotud nõuete täitmist. Samas tuleb märkida, et rikkumisest teatamata jätmine kas üksikisikule või järelevalveasutusele võib tähendada, et vastutavale töötajale määratakse artikli 83 alusel karistus.

Vastutavaid töötlejaid ja volitatud töötlejaid julgustatakse seetõttu tegema ettevalmistusi ja kehtestama menetlused, et olla suuteline rikkumisi avastama, need kohe peatama ja hindama

---

[1] Vt isikuandmete kaitse üldmääruse artikli 4 lõige 21

[2] Vt http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:32009L0136 ja http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32013R0611

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

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

[5] Euroopa Liidu põhiõiguste hartas sätestatud õigused, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] Vt artikli 33 lõige 2. See on sarnane määruse (EL) nr 611/2013 artikliga 5, milles on kehtestatud, 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.

[7] Vt artikli 34 lõige 4 ja artikli 58 lõike 2 punkt e.

üksikisikutele avalduvat ohtu[8], ning seejärel tegema kindlaks, kas pädevat järelevalveasutust on vaja teavitada, ning vajaduse korral teavitama rikkumisest asjaomaseid üksikisikuid. Järelevalveasutuste teavitamine peaks olema juhtumi lahendamise plaani osa.

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.

Oma arvamuses 03/2014 isikuandmetega seotud rikkumistest teatamise kohta[9] esitas artikli 29 töörühm juhised vastutavatele töötlejatele, et aidata neil otsustada, kas teavitada rikkumisest andmesubjekte. Arvamuses käsitleti elektrooniliste sideteenuste osutajate kohustust seoses direktiiviga 2002/58/EÜ ning esitati kõikidele vastutavatele töötlejatele tol hetkel isikuandmete kaitse üldmääruse eelnõu valguses näiteid ja parimaid tavasid erinevatest sektoritest.

Kehtivates suunistes selgitatakse isikuandmete kaitse üldmäärusest tulenevaid kohustuslikke rikkumisest teavitamise ja suhtlemise nõudeid ning mõningaid samme, mida vastutavad töötlejad ja volitatud töötlejad saavad astuda uute kohustuste täitmiseks. Samuti esitatakse näiteid erinevate rikkumiste kohta ning selle kohta, keda tuleks erinevate juhtumite korral teavitada.

I. Isikuandmetega seotud rikkumisest teatamine isikuandmete kaitse üldmääruse alusel

A. Peamised turvakaalutlused

Isikuandmete kaitse üldmääruse üks nõuetest kehtestab, 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[10].

Sellest tulenevalt nõutakse isikuandmete kaitse üldmääruses, et nii vastutavad töötlejad kui ka volitatud töötlejad kehtestavad ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. 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[11]. 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 teavitamise kohustus[12].

Sellest tulenevalt on mis tahes andmeturbepoliitika üks peamisi ülesandeid olla suuteline võimaluse korral rikkumisi ära hoidma ja kui need siiski esinevad, reageerida nendele õigeaegselt.

---

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

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

[10] Artikli 5 lõike 1 punkt f ja artikkel 32.

[11] Artikkel 32; vt ka põhjendus 83

[12] Vt põhjendus 87

A.

B. Mis on isikuandmetega seotud rikkumine?

1. Mõiste

Selleks et vastutav töötleja saaks rikkumist käsitleda, tuleb tal see ära tunda. Isikuandmete kaitse üldmääruse artikli 4 lõikes 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.“

Mida mõeldakse isikuandmete „hävitamise“ all, peaks olema üsna selge: see on olukord, kui andmeid enam ei eksisteeri või ei eksisteeri sellises vormingus, mida vastutav töötleja saaks kasutada. „Kahju“ mõiste peaks olema samuti üsna arusaadav: olukord, kui 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. Viimaseks, loata või ebaseaduslik töötlemine võib tähendada seda, et isikuandmeid avaldavad (või võimaldavad nendele juurdepääsu) isikud, kellel ei ole luba neid andmeid vastu võtta (nendele juurde pääseda), või töödeldakse andmeid mis tahes muul viisil, mis rikub isikuandmete kaitse üldmäärust.

Näide

Isikuandmete kaotsiminek esineb näiteks siis, kui seade, kuhu on salvestatud vastutava töötleja klientide andmebaas, on kaotatud või varastatud. Veel üks näide kaotsiminekust on olukord, kus lunavara on krüpteerinud isikuandmete ainukoopia, või kui vastutav töötleja on koopia krüpteerinud võtmega, mis enam ei ole tema valduses.

Oluline on siinkohal see, et rikkumine on turvaintsidendi üks liikidest. Kuid nagu on osutatud artikli 4 lõikes 12 kohaldub isikuandmete kaitse üldmäärus üksnes siis, kui esineb *isikuandmetega* seotud rikkumine. Sellise rikkumise tulemusel ei suuda vastutav töötleja tagada vastavust isikuandmete kaitse üldmääruse artiklis 5 esitatud isikuandmete töötlemise põhimõtetega. Siit tuleb välja erinevus turvaintsidendi ja isikuandmetega seotud rikkumise vahel – sisuliselt on kõik isikuandmetega seotud rikkumised turvaintsidendid, kuid kõik turvaintsidendid ei ole tingimata isikuandmetega seotud rikkumised[13].

Rikkumise võimalikku kahjulikku mõju üksikisikutele arutatakse allpool.

2. Isikuandmetega seotud rikkumiste liigid

Artikli 29 töörühm selgitas oma arvamuses 03/2014 rikkumisest teatamise kohta, et rikkumisi võib jaotada kategooriatesse vastavalt järgmisele kolmele hästituntud infoturbe põhimõttele[14]:

- „Konfidentsiaalsusega seotud rikkumine“ – isikuandmete loata või juhuslik avalikustamine või neile juurdepääs.
- „Terviklusega seotud rikkumine“ – isikuandmete loata või juhuslik muutmine.

[13] Tuleb märkida, et turvaintsident ei piirdu ohumudelitega, kui organisatsiooni rünnatakse välisest allikast, vaid hõlmab asutusesiseseid töötlemisintsidente, millega rikutakse turvalisuse põhimõtteid.

[14] Vt arvamus 03/2014

- „Kättesaadavusega seotud rikkumine“ – isikuandmetele juurdepääsu juhuslik või loata kaotsiminek[15] või hävitamine.

Samuti tuleb märkida, et olenevalt olukorrast võib rikkumine olla seotud samal ajal isikuandmete konfidentsiaalsuse, tervikluse ja kättesaadavusega või nende erinevate kombinatsioonidega.

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

Näide

Kättesaadavuse kaotsimineku näidete hulka kuulub olukord, kui andmed on kogemata kustutatud või on seda teinud 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 alaliseks kaotsiminekuks.

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

Võib küsida, kas isikuandmete ajutist kättesaadavuse kaotsiminekut võib pidada rikkumiseks ning kui saab, siis kas sellest tuleb teada anda. Isikuandmete kaitse üldmääruse artiklis 32 „Töötlemise turvalisus“ selgitatakse, et kui rakendatakse tehnilisi ja korralduslikke meetmeid, et tagada ohule vastav turvalisuse tase, tuleb arvestada muu hulgas „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“.

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 artikli 4 lõikes 12.

Kui isikuandmed lähevad kaotsi või hävitatakse alaliselt (või kui tegemist on ükskõik millise muu rikkumisega), tuleb kättesaadavuse ajutine kaotsiminek dokumenteerida kooskõlas artikli 33 lõike 5 nõuetega. Seeläbi saab vastutav töötleja näidata üles vastutust järelevalveasutuse ees, kes võib neid dokumente[16] näha soovida. Kuid olenevalt rikkumise asjaoludest, võib järelevalveasutuse teavitamine ning mõjutatud isikutega suhtlemine olla vajalik/tarbetu. Vastutav töötleja peab hindama, kui tõenäoliselt ja tõsiselt mõjutab isikuandmete kättesaadavusse puudumine füüsiliste isikute õigusi ja vabadusi. Kooskõlas artikliga 33 peab vastutav töötleja rikkumisest teatama, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Kahtlemata tuleb olukorda hinnata iga juhtumi puhul eraldi.

[15] See on hästijuurdunud teadmine, et „juurdepääs“ on põhimõtteliselt osa „kättesaadavusest“. Vaata näiteks, NIST SP800-53rev4, 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 määratleb „kättesaadavuse“ samuti kui „Teabe, millele volitatud üksusel on juurdepääs ja mida ta saab nõudmise korral kasutada“: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] Vt artikli 33 lõige 5.

Näited

Haigla – kui patsientide kriitilised terviseandmed ei ole kättesaadavad kasvõi ajutiselt, võib see kujutada ohtu üksikisikute õigustele ja vabadustele. Näiteks tekib vajadus operatsioonid tühistada ja sellega seatakse elud ohtu.

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

Tuleb märkida, et ehkki vastutava töötaja süsteemide kättesaadavuse kaotsiminek võib olla ajutine ja ei mõjuta üksikisikuid, on oluline, et vastutav töötleja kaalub kõiki rikkumise võimalikke tagajärgi, sest teavitamine võib olla vajalik teistel põhjustel.

Näide

Nakatumisel lunavaraga (pahavara, mis krüpteerib vastutava töötleja andmed kuni lunaraha maksmiseni) võib tekkida kättesaadavuse ajutine kaotsiminek, kui andmed saab taastada varukoopiast. Kuid võrgustikku on siiski sisse tungitud ja teavitamine võib olla vajalik, kui intsident kvalifitseerub konfidentsiaalsusega seotud rikkumisena (st ründaja pääseb juurde isikuandmetele) ning seab ohtu üksikisikute õigused ja vabadused.

3. Isikuandmetega seotud rikkumise võimalikud tagajärjed

Rikkumine võib üksikisikuid kahjulikult mõjutada mitmel viisil ja selle tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju. Isikuandmete kaitse üldmääruses selgitatakse, et see võib hõlmata kontrolli kaotamist oma isikuandmete üle või õiguste piiramist, diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, pseudonümiseerimise loata tühistamist, maine kahjustamist, ametisaladusega kaitstud andmete konfidentsiaalsuse kadu. Samuti võib see hõlmata muud tõsist majanduslikku või sotsiaalset kahju asjaomastele füüsilistele isikutele[17].

Seetõttu nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja teavitab rikkumisest pädevat järelevalveasutust, välja arvatud, kui rikkumisest tuleneva kahjuliku mõju oht on ebatõenäoline. Kui kahjuliku mõju esinemise oht on tõenäoliselt suur, nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja teavitab rikkumisest mõjutatud üksikisikuid nii kiiresti kui mõistlikkuse piires võimalik[18].

Isikuandmete kaitse üldmääruse artiklis 87 rõhutatakse, kui oluline on suuta rikkumine tuvastada, hinnata selle ohtu üksikisikutele ja sellest vajaduse korral teada anda:

„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.“

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

[17] Vt ka põhjendused 85 ja 75.

[18] Vt ka põhjendus 86.

Kui vastutavad töötlejad ei teata andmete rikkumisest ei järelevalveasutusele ega andmesubjektidele või mõlematele, olgugi et artikli 33 ja/või 34 nõuded on täidetud, tuleb järelevalveasutusel kaaluda kõiki tema käsutuses olevaid parandusmeetmeid ja sealhulgas kaaluda vajadust määrata asjakohane trahv[19] kas koos artikli 58 lõike 2 kohase parandusmeetmega või iseseisvalt. Kui otsustatakse määrata trahv, võib selle suurus vastavalt isikuandmete kaitse üldmääruse artikli 83 lõike 4 punkti a kohaselt olla kuni 10 000 000 eurot või ettevõtja puhul kuni 2 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest. Samuti on oluline pidada meeles, et teatud juhtudel võib teatamata jätmine näidata, et turvameetmed puuduvad või on kehtivad turvameetmed puudulikud. Artikli 29 töörühma suunistes trahvide kohta on öeldud: „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 (artiklid 33 ja 34) ja teiselt poolt (piisavate) turvameetmete puudumise eest (artikkel 32), kuna tegemist on kahe erineva rikkumisega.

II. Artikkel 33 - Järelevalveasutuse teavitamine

A. Millal teatada

1. Artikli 33 nõuded

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.“

Põhjenduses 87[20] on kirjas:

> „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“?

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

[19] Täiendavaid üksikasju vaadake palun artikli 29 töörühma suuniseid trahvide kohaldamise ja määramise kohta: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

[20] Põhjendus 85 on siinkohal samuti oluline.

töötleja on saanud rikkumisest „teada“. Artikli 29 töörühm leiab, et vastutav töötleja on saanud rikkumisest „teada“, kuid ta on mõistlikul määral kindel, et toimunud on turvaintsident, mille tulemusel on isikuandmete kaitstus rikutud.

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[21]. See seab vastutavale töötlejale kohustuse tagada, et nad saavad mis tahes rikkumistest „teada“ õigeaegselt, et nad saaksid astuda asjakohaseid samme.

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

Näited

1. Krüpteerimata isikuandmetega USB-mälupulga kaotamise korral ei ole sageli võimalik kindlaks teha, kas volitamata isikutel oli andmetele juurdepääs. Isegi kui vastutav töötleja ei ole suuteline kindlaks tegema, kas konfidentsiaalsusega seotud rikkumine on toimunud, tuleb sellisest juhtumist siiski teada anda, kuna piisava kindlusega saab 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 nad on juhuslikult saanud ühe töötleja 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 võrgustikku. Vastutav töötleja kontrollib oma süsteeme, et teha kindlaks, kas süsteemis talletatud isikuandmete kaitstus on rikutud, ning saab selle kohta kinnituse. Jällegi, kuna vastutaval töötlejal on selged tõendid rikkumise kohta, ei ole kahtlust, et ta on rikkumisest „teada“ saanud.

4. Küberkurjategija võtab pärast süsteemi häkkimist vastutava töötlejaga ühendust, et lunaraha nõuda. Sellisel juhul on vastutaval töötlejal pärast süsteemi kontrollimist ja kinnituse saamist selle ründamise kohta kindlad tõendid, et rikkumine on toimunud, ning ei ole kahtlustki, et vastutav töötleja on saanud sellest teada.

Pärast võimaliku rikkumise kohta teabe 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 sel perioodil ei saa väita, et vastutav töötleja on rikkumisest „teada“ saanud. Siiski eeldatakse, et esialgse uurimisega alustatakse võimalikult vara ning tuvastatakse piisava kindlusega, kas rikkumine on toime pandud; seejärel võib korraldada põhjalikuma uurimise.

[21] Vt põhjendus 87

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 üksikisikutele avalduda võivat ohtu, et teha kindlaks, kas on tekkinud teavitamise 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[22] raames enne asjaomase töötlemisoperatsiooni korraldamist. Kuid andmekaitsealane mõjuhinnang võib siiski olla üldisem võrreldes tegeliku rikkumise konkreetsete asjaoludega ja seega tuleb igal juhul teha täiendav hinnang, milles võetakse arvesse konkreetseid asjaolusid. Üksikasjalikumat teavet ohu hindamise kohta vaadake IV jaost.

Enamikel juhtudel tuleks esialgsete tegevustega alustada kohe pärast esimest hoiatust (st kui vastutav töötleja või volitatud töötleja kahtlustab, et toimunud on turvaintsident, mis võib hõlmata isikuandmeid). Vaid erakorraliste juhtumite puhul võib selleks rohkem aega minna.

Näide

Üksikisik teavitab vastutavat töötlejat, et ta on saanud vastutava töötleja nimel e-kirja, mis sisaldab isikuandmeid vastutava töötleja pakutud teenuse temapoolse (tegeliku) kasutamise kohta, oletades, et vastutava töötleja andmete turvalisust on rikutud. Vastutav töötleja korraldab lühiajalise uurimise ja teeb kindlaks, et tema võrgustikku on sisse tungitud, ja leiab tõendeid isikuandmetele loata juurdepääsu kohta. Nüüd võib öelda, et vastutav töötleja on saanud „teada“ ja sellest tuleb teavitada järelevalveasutust, välja arvatud juhul, kui see ei kujuta endast tõenäoliselt ohtu üksikisikute õigustele ja vabadustele. Vastutav töötleja peab võtma rikkumisega tegelemiseks sobivad parandusmeetmed.

Seega peab vastutaval töötlejal olema kehtestatud ettevõttesisesed menetlused rikkumiste avastamiseks ja käsitlemiseks. Näiteks, kõrvalekallete leidmiseks andmetöötluses võib vastutav töötleja või volitatud töötleja kasutada selliseid tehnilisi meetmeid nagu andmevoo- ja logianalüsaatorid, mille abil on võimalik määratleda sündmusi ja hoiatusi mis tahes logiandmeid seostades[23]. On oluline, et rikkumise avastamise korral edastatakse teade asjakohase kõrgemalseisva juhtimistasandini, et rikkumisega saaks tegeleda ja vajaduse korral sellest teada anda kooskõlas artikliga 33 ja vajaduse korral artikliga 34. Selliseid meetmeid ja aruandlusmehhanisme võib üksikasjalikult kirjeldada vastutava töötleja intsidentidele reageerimise kavades ja/või intsidentide juhtimiskorras. Nende abil saab vastutav töötleja paremini tulemuslikult kavandada ja teha kindlaks organisatsioonisisese vastutuse rikkumise lahendamise juhtimise eest ning kuidas või kas viia vajaduse korral selle lahendamine kõrgemale juhtimistasemele.

Vastutaval töötlejal peaks samuti olema kehtestatud kord seoses volitatud töötlejatega, keda vastutav töötleja kasutab; volitatud töötlejal on omakorda kohustus teavitada vastutavat töötlejat rikkumise esinemisel (vt allpool).

Ehkki rikkumise tõkestamiseks, sellele reageerimiseks ja sellega tegelemiseks sobilike meetmete kehtestamise vastutus lasub vastutavatel töötlejatel ja volitatud töötlejatel, on mõned praktilised sammud, mida tuleb astuda igal juhul.

- Kogu turvalisusega seotud juhtumite teave tuleb suunata vastutavale isikule või isikutele, kellel on ülesanne tegeleda intsidentidega, teha kindlaks rikkumise esinemine ja hinnata ohtu.

[22] Vt artikli 29 töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[23] Tuleb märkida, et nt andmete salvestamise, muutmise või kustutamise auditeerimist hõlbustavad logiandmed võivad samuti kvalifitseeruda vastava töötlemistoimingu algatanud isiku isikuandmeteks.

- Rikkumisel tulemusel üksikisikutele avalduvat ohtu tuleb seejärel hinnata (tõenäosus, et ohtu ei ole, oht esineb või oht on suur) ja teavitada organisatsiooni asjaomaseid osakondi.
- Teavitada tuleb järelevalveasutust ning vajaduse korral tuleb teade rikkumise kohta edastada mõjutatud üksikisikutele.
- Samal ajal peab vastutav töötleja tegutsema rikkumise leviku piiramiseks ja esialgse olukorra taastamiseks.
- Rikkumine tuleb dokumenteerida vastavalt selle arengule.

Seega peaks olema selge, et vastutaval töötlejal on kohustus tegutseda kõikide esialgsete hoiatuste puhul ja teha kindlaks, kas rikkumine on tegelikult toimunud või mitte. Selle lühikese aja jooksul saab teha põgusa uurimise ning vastutav töötleja saab koguda tõendeid ja muid asjassepuutuvaid üksikasju. Ent kui vastutav töötleja on piisava kindlusega tuvastanud, et rikkumine on toime pandud, ehk kui artikli 33 lõike 1 tingimused on täidetud, peab ta sellest teavitama järelevalveasutust põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul[24]. Kui vastutav töötleja ei tegutse õigeaegselt ja selgub, et rikkumine on toime pandud, võib seda pidada artiklil 33 kohaseks teatamata jätmiseks.

Artiklis 32 on selgelt öeldud, et vastutav töötleja ja volitatud töötleja rakendavad ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid: võimet rikkumine avastada, sellega tegeleda ja sellest õigel ajal teada anda tuleks pidada nende meetmete oluliseks osaks.

3. Kaasvastutavad töötlejad

Artiklis 26 käsitletakse kaasvastutavaid töötlejaid ning täpsustatakse, et kaasvastutavad töötlejad määravad oma asjaomase vastutusvaldkonna isikuandmete kaitse üldmääruse täitmiseks[25]. See tähendab, et määratakse kindlaks kumb osapool vastutab artiklite 33 ja 34 kohaste kohustuste täitmise eest. Artikli 29 töörühm soovitab, et lepingupõhised kokkulepped kaasvastutajate vahel sisaldaks sätteid, millega määratakse kindlaks, kumb kaasvastutajatest on vastutav isikuandmete kaitse üldmääruses kehtestatud rikkumisteate edastamise eest.

4. Volitatud töötleja kohustused

Isikuandmete kaitse ees säilitab vastutuse vastutav töötleja, kuid volitatud töötlejal on täita oluline roll, et võimaldada vastutaval töötlejal oma kohustusi täita; ning nende hulka kuulub rikkumisest teatamine. Artikli 28 lõikes 3 täpsustatakse, 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“.

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. Tuleb märkida, et volitatud töötleja ei pea enne vastutava töötleja teavitamist kõigepealt hindama rikkumisest tuleneva ohu tõenäosust; selle hinnangu peab tegema vastutav töötleja rikkumisest teada saamisel. Volitatud töötleja peab vaid 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 „teada“, kui volitatud töötleja on

[24] 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=EN

[25] Vt ka põhjendus 79.

teda rikkumisest teavitanud. Volitatud töötleja kohustus vastutavat töötlejat teavitada võimaldab vastutaval töötlejal rikkumisega tegeleda ja teha kindlaks, kas ta peab / 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 positsioon ei võimalda tal teada kõiki teemaga seotud asjaolusid, näiteks kui vastutaval töötlejal on endiselt alles koopia või varukoopia isikuandmetest, mille volitatud töötleja hävitas või kaotas. See asjaolu võib otsustada, kas vastutav töötleja peab sellest teada andma.

Isikuandmete kaitse üldmääruses ei ole kehtestatud selgesõnalist ajapiiri, mille jooksul volitatud töötleja peab vastutavat töötlejat hoiatama, välja arvatud juhud, millal tuleb seda teha „põhjendamatu viivituseta“. Seetõttu soovitab artikli 29 töörühm, 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.

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.

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

Volitatud töötleja võib teavitada vastutava töötleja nimel, kui vastutav töötleja on volitatud töötlejale andnud asjakohase volituse ja see on osa vastutava töötleja ja volitatud töötleja vahelistest lepingupõhistest kokkulepetest. Selline teavitamine peab toimuma kooskõlas artiklitega 33 ja 34. Siiski on oluline märkida, et õiguslik vastutus teavitamise eest on endiselt vastutaval töötlejal.

B. Järelevalveasutuse teavitamine

1. Esitatav teave

Kui vastutav töötleja teavitab järelevalveasutust rikkumisest, tuleb 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 asjaomaste isikuandmekirjete 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.“

Isikuandmete kaitse üldmääruses ei ole andmesubjektide kategooriaid ega isikuandmekirjete liike määratletud. Artikli 29 töörühm teeb siiski soovituse andmesubjektide kategooriate kohta, et osutada üksikisikute erinevatele liikidele, kelle isikuandmeid rikkumine on mõjutanud: olenevalt kasutatud deskriptoritest võib see hõlmata muu hulgas lapsi ja teisi haavatavaid rühmi, puuetega inimesi, töötajaid või kliente. Samamoodi võivad isikuandmekirjete liigid osutada erinevat liiki kirjetele, mida vastutav töötleja võib töödelda, näiteks terviseandmed, hariduskirjed, sotsiaalhoolekande teave, finantsandmed, pangakontonumbrid, passinumbrid jne.

Põhjenduses 85 selgitatakse, et teatamise üks eesmärkidest on vähendada üksikisikutele tekkivat kahju. Sellest tulenevalt, kui andmesubjektide kategooriatest või isikuandmete liikidest nähtub, et rikkumise tulemusel tekib teatav oht (nt identiteedivargus, pettus, rahaline kaotus, oht ametisaladusele), siis on oluline, et teavitamisel märgitakse need kategooriad ära. Sel moel on see seotud nõudega kirjeldada rikkumise võimalikke tagajärgi.

Kui täpset teavet ei ole (nt mõjutatud andmesubjektide täpset arvu), ei tohiks see olla takistuseks rikkumisest õigel ajal teavitada. Isikuandmete kaitse üldmäärusega lubatakse esitada mõjutatud üksikisikute ja isikuandmekirjete ligikaudne arv. Täpsete näitajate esitamise asemel peaks tähelepanu keskmes olema rikkumise kahjulik mõju. Seega, kui on selge, et rikkumine on toimunud, kuid selle ulatus ei ole veel teada, on järkjärguline teavitamine (vt allpool) kindel viis teatamise kohustuse täitmiseks.

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

Näide

Osana järelevalveasutuse teavitamisest võib vastutav töötleja pidada kasulikuks ära märkida volitatud töötleja, kui tema on rikkumise peamine põhjus, eriti kui seetõttu toimub intsident, mis mõjutab sama volitatud töötlejat kasutavate teiste vastutavate töötlejate isikuandmekirjeid.

Igal juhul võib järelevalveasutus rikkumise uurimise raames nõuda täiendavaid üksikasju.

2. Järkjärguline teatamine

Olenevalt rikkumise laadist võib vastutava töötleja poolne täiendav uurimine olla vajalik, et teha kindlaks kõik intsidendiga seotud faktid. 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.“

See tähendab, et isikuandmete kaitse üldmääruses tunnistatakse, et vastutavatel töötlejatel ei ole alati kogu teavet rikkumise kohta 72 tunni jooksul pärast rikkumisest teada saamist, kuna intsidendi kõik üksikasjad ei pruugi kohe alguses kättesaadavad olla. Seega lubatakse teavet edastada järk-järgult. Tõenäolisemalt esineb selline olukord keerukamate rikkumiste puhul, nagu küberjulgeoleku intsidentide teatud liigid, mille puhul võib osutuda vajalikuks põhjaliku kohtuekspertiisi tegemine, et määrata täielikult kindlaks rikkumise laad ja ulatus, mil määral isikuandmete kaitstus on rikutud. Sellest tulenevalt tuleb vastutaval töötlejal paljudel juhtudel hiljem teha ulatuslikum uurimine ja võtta järelmeetmed täiendava teabe alusel. See on lubatud, kui vastutav töötleja esitab viivituse põhjused kooskõlas artikli 33 lõikega 1. Artikli 29 töörühm soovitab, et kui vastutav töötleja teavitab järelevalveasutust esimest korda, annab vastutav töötleja järelevalveasutusele teada, et tal ei ole veel kogu vajalikku teavet ja ta esitab täiendavad üksikasjad hiljem. Järelevalveasutus kinnitab kuidas ja millal lisateave tuleb esitada. See ei takista vastutaval töötlejal lisateavet esitamast järgmistes etappides, kui ta saab teada täiendavatest rikkumisega seotud üksikasjadest, mis tuleb järelevalveasutusele edastada.

Rikkumisest teatamise nõude eesmärk on innustada vastutavaid töötlejaid rikkumise esinemisel kohe tegutsema, piirama selle levikut ja võimaluse korral taastama ohtu sattunud isikuandmed ning otsima asjakohast abi järelevalveasutuselt. Järelevalveasutuse esmakordne teavitamine 72 tunni jooksul võimaldab vastutaval töötlejal tagada, et üksikisikute teavitamisega/mitteteavitamisega seotud otsused on õiged.

Järelevalveasutuse teavitamise eesmärk ei ole siiski saada üksnes 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 erikategooriad[26] avalikustatakse veebis, tuleb vastutaval töötlejal tegutseda põhjendamatu viivituseta, et piirata rikkumise levik ja teavitada sellest asjaomaseid üksikisikuid (vt III jagu). Erandkorras võib see toimuda isegi enne järelevalveasutuse teavitamist. Üldisemalt, järelevalveasutuse teavitamist ei saa kasutada õigustusena, kui nõuetekohane rikkumisteade jäetakse andmesubjektidele edastamata.

Samuti peaks olema selge, et pärast esialgse teate edastamist saadab vastutav töötleja järelevalveasutusele uut teavet, kui hilisema uurimise käigus leitakse tõendeid, et turvaintsidendi ulatusele pandi piir ja rikkumist tegelikult ei toimunud. Selle teabe võib lisada teabele, mis järelevalveasutusele juba edastati, ning intsidenti ei registreerita rikkumisena. Sellise intsidendist teavitamist, mille lõpuks selgub, et tegemist ei olnud rikkumisega, ei karistata.

Näide

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

Tuleb märkida, et järkjärguline lähenemisviis teatamisele on juba kehtestatud direktiivis 2002/58/EÜ, määruses 611/2013 ja teiste automaatteavitusega intsidentide puhul.

3. Hilinenud teatamine

Artikli 33 lõikes 1 selgitatakse, et kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus. Nii see kui ka järkjärgulise teatamise kontseptsioon annavad tunnistust, et vastutav töötleja ei pruugi alati suuta rikkumisest teavitada etteantud aja jooksul ning hilinenud teavitamine võib olla lubatud.

Selline olukord võib tekkida näiteks siis, kui vastutaval töötlejal esineb lühikese aja jooksul mitu sarnast konfidentsiaalsusega seotud rikkumist, mis mõjutavad väga paljusid andmesubjekte samal viisil. Vastutav töötleja võib saada rikkumisest teada ning uurimist alustades, kuid enne teavitamist võib avastada sarnaseid rikkumisi, millel on teised põhjused. Olenevalt tingimustest võib vastutaval töötlejal kuluda rikkumiste ulatuse kindlakstegemiseks 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 esimest korda sai rikkumistest teada.

Rangelt võttes tuleb igast üksikust rikkumisest teavitada. Ülekoormuse vältimiseks võib vastutav töötleja esitada koondteate, mis kajastab kõiki asjaomaseid rikkumisi, tingimusel et need kõik on samaliigiliste isikuandmete samalaadsed rikkumised, mis esinesid suhteliselt lühikese aja jooksul. Kui toimub mitu rikkumist, mis on seotud isikuandmete eriliikidega, mida rikutakse erineval viisil, tuleb teavitamine korraldada tavapärasel viisil ehk igast rikkumisest teavitatakse kooskõlas artikliga 33.

Ehkki isikuandmete kaitse üldmäärusega on hilinenud teavitamine mingil 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.

[26] Vt artikkel 9.

C. Piiriülesed rikkumised ja rikkumised ELi-välistes asutustes

1. Piiriülesed rikkumised

Kui toimub isikuandmete piiriülene rikkumine[27], võib see mõjutada andmesubjekte rohkem kui ühes liikmesriigis. Artikli 33 lõikes 1 on selgelt öeldud, et rikkumise korral teavitab vastutav töötleja isikuandmetega seotud rikkumisest isikuandmete kaitse üldmääruse[28] artikli 55 kohast pädevat järelevalveasutust. Artikli 55 lõikes 1 on öeldud:

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

Kuid artikli 56 lõikes 1 on öeldud:

> „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 piirülese isikuandmete töötlemise toimingu suhtes kooskõlas artiklis 60 sätestatud menetlusega."

Lisaks on artikli 56 lõikes 6 öeldud:

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

See tähendab, et kui rikkumine toimub andmete piiriülese töötlemise käigus ja sellest tuleb teavitada, peab vastutav töötleja teavitama juhtivat järelevalveasutust[29]. Seega, peab vastutav töötleja rikkumise lahendamise kava koostades hindama, milline järelevalveasutus on juhtiv järelevalveasutus, keda tuleb rikkumisest teavitada[30]. 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, mis ei ole tingimata see koht, 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 juhtiva järelevalveasutuse kindlaksmääramisel, tuleks tal teavitada vähemalt seda kohalikku järelevalveasutust, kus rikkumine toimus.

2. Rikkumised ELi-välistes asutustes

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 artikli 3 lõikes 2 öeldud[31]:

---

[27] Vt artikli 4 lõige 23.

[28] Vt ka põhjendus 122.

[29] Vt artikli 29 töörühma *Vastutava töötleja või volitatud töötleja juhtiva järelevalveasutuse kindlaksmääramise suunised* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

[30] Kõikide Euroopa riiklike andmekaitseametite kontaktandmete loetelu leiate aadressil: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Vt ka põhjendused 23 ja 24

„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.“

Samuti on asjakohane artikli 3 lõige 3, kus on öeldud[32]:

„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.“

Kui mujal kui liidus asuva vastutava töötleja suhtes kohaldatakse artikli 3 lõiget 2 või 3 ning tema ettevõttes toimub rikkumine, kehtib seega tema suhtes endiselt artiklitest 33 ja 34 tulenev teavitamise kohustus. Artiklis 27 on nõutud, kui kohaldatakse artikli 3 lõiget 2, siis määrab vastutav töötleja (ja volitatud töötleja) oma esindaja liidus. Sellistel juhtudel soovitab artikli 29 töörühm, et teade esitatakse järelevalveasutusele liikmesriigis, kus vastutava töötleja esindaja liidus on määratud[33]. Samamoodi, kui volitatud töötleja suhtes kohaldatakse artikli 3 lõiget 2, on ta seotud volitatud töötlejate suhtes kehtiva kohustusega teavitada rikkumisest vastutavat töötlejat vastavalt artikli 33 lõikele 2, mis siinkohal on eriti oluline.

D. Tingimused, kui teavitamine ei ole vajalik

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 vastupidine direktiivis 2009/136/EÜ sätestatud rikkumisest teatamise nõuetega, mis kehtivad üldkasutatavate elektrooniliste sideteenuste osutajate suhtes ja mille kohaselt tuleb pädevale asutusele teatada kõikidest asjaomastest rikkumistest.

Oma arvamuses 03/2014 rikkumisest teatamise kohta[34] selgitas artikli 29 töörühm, et konfidentsiaalsusega seotud rikkumine, kus isikuandmed on krüpteeritud uusima teadusliku algoritmi alusel, on ikkagi isikuandmetega seotud rikkumine ja sellest tuleb teavitada. Kui võtme konfidentsiaalsus on siiski terviklik, st võtme kaitstust ei rikutud ühegi turvanõuete rikkumise käigus, ning võti loodi selliselt, et seda ei saa ühegi olemasoleva tehnilise vahendiga kindlaks teha ükski isik, on andmed põhimõtteliselt loetamatud. Seega ei avalda rikkumine tõenäoliselt üksikisikutele kahjulikku mõju ja seetõttu ei ole vaja neile sellest teatada[35]. Kuid, 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 nõutud, olgugi et andmete suhtes kohaldati piisavaid krüpteerimismeetmeid.

---

[32] Vt ka põhjendus 25

[33] Vt põhjendust 80 ja artiklit 27

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

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

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 kaitstust 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.

Sellest tulenevalt, kui isikuandmed on volitamata isikutele põhimõtteliselt muudetud loetamatuks ja kui andmetest on koopia või varukoopia, ei pruugi tekkida vajadust teavitada järelevalveasutust nõuetekohaselt krüpteeritud isikuandmete konfidentsiaalsusega seotud rikkumisest. Seda seetõttu, et selline rikkumine tõenäoliselt ei põhjusta ohtu üksikisikute „õigustele ja vabadustele“. See tähendab seda, et puudub ka vajadus teavitada asjaomast üksikisikut, kuna suure ohu tõenäosus on madal. Siiski tuleb meeles pidada, et kuna alguses puudub vajadus teavitada, sest tõenäolist ohtu üksikisikute õigustele ja vabadustele ei ole, võib see aja jooksul muutuda ning ohu suurust tuleb uuesti hinnata. Näiteks, kui seejärel leitakse, et võtme kaitstus on ohustatud või krüpteerimistarkvaras leitakse turvaauk, võib teate saatmine siiski vajalik olla.

Lisaks tuleb märkida, et kui krüpteeritud isikuandmed ei ole varundatud ja toimub rikkumine, siis on toimunud kättesaadavusega seotud rikkumine, mis põhjustab ohtu üksikisikutele ja seega võib teavitamine osutuda vajalikuks. Samamoodi, kui toimub rikkumine, mille käigus lähevad krüpteeritud andmed kaotsi, ning olgugi et isikuandmete varukoopia on olemas, võib endiselt olla tegemist teavitamist vajava rikkumisega, olenevalt sellest, kui palju aega kulub varukoopiast andmete taastamiseks ja kuidas andmete kättesaadavuse puudumine mõjutab üksikisikuid. Nagu artikli 32 lõike 1 punktis c on öeldud, turvalisuse oluline tegur on „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 ja vabadustele. Kui hiljem selgub, et krüpteerimisvõtme kaitstus on rikutud või et krüpteerimistarkvaras või algoritmis on turvaauk, muutub üksikisikute õiguste ja vabadustele avalduva ohu suurus ja teavitamine võib nüüd osutuda vajalikuks.

Artikli 33 nõuded on siiski täitmata, kui vastutav töötleja ei teavita järelevalveasutust olukorras, kus andmeid ei ole tegelikult turvaliselt krüpteeritud. Seega peaksid vastutavad töötlejad krüpteerimistarkvara valimisel hoolikalt kaaluma pakutava krüpteerimisteenuse kvaliteeti ja nõuetekohast rakendamist, mõistma, millise taseme kaitset tegelikult pakutakse ja kas see on piisav esinevate ohtude puhul. Vastutavad töötlejad peaksid samuti olema tuttavad nende käsutuses oleva krüpteerimistoote toimimise eripäradega. Näiteks toimub seadme krüpteerimine selle väljalülitamisel, kuid mitte ooterežiimis. Osadel krüpteerimist kasutavatel toodetel on nn vaikimisi klahvid, mida krüpteeringu tagamiseks tuleb igal kasutajal muuta. Turvaeksperdid võivad krüpteerimist praegu pidada piisavaks, kuid see võib mõne aasta pärast olla vananenud, ehk on kaheldav, kas see toode suudab andmeid piisavalt krüpteerida ja pakkuda nõuetekohast kaitset.

III. **Artikkel 34 – Andmesubjekti teavitamine**

A. Üksikisikute teavitamine

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

Artikli 34 lõikes 1 on sätestatud:

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

Vastutavad töötlejad peaksid meeles pidama, et järelevalveasutuse teavitamine on kohustuslik, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele. Lisaks sellele tuleb teavitada samuti üksikisikuid, kui rikkumise tõttu võivad üksikisikute õigused ja vabadused suurde ohtu sattuda. Seetõttu on üksikisikutele rikkumisest teavitamise lävend kõrgem kui järelevalveasutuste puhul ning seega ei ole kõikidest rikkumistest üksikisikuid vaja teavitada, kaitstes neid tarbetu teavitamisväsimuse eest.

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 sammude kohta, mida nad saavad enda kaitseks astuda[36]. Nagu märgitud eespool, võib õigeaegne teavitamine olenevalt rikkumise ja tekkinud ohu laadist aidata üksikisikutel end kaitsta rikkumise kahjulike tagajärgede eest.

Käesolevate suuniste lisas B on esitatud mittetäielik nimekiri näidetest, millal rikkumisest võib tuleneda suur oht üksikisikutele, ja sellest tulenevatest olukordadest, millal vastutav töötleja peab rikkumisest teavitama mõjutatud isikuid.

B. Esitatav teave

Üksikisikute teavitamise kohta on 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.“

Selle sätte kohaselt peaks vastutav töötleja esitama vähemalt järgmise teabe:

- rikkumise laadi kirjeldus;
- andmekaitseametniku või mõne teise kontaktisiku nimi ja kontaktandmed;
- rikkumise võimalike tagajärgede kirjeldus ning
- rikkumise lahendamiseks vastutava töötleja poolt võetud või võtmiseks kavandatud meetmete kirjeldus, sealhulgas vajaduse korral meetmed rikkumise võimaliku kahjuliku mõju leevendamiseks.

Näitena meetmetest, mis on võetud rikkumise lahendamiseks ja võimaliku kahjuliku mõju leevendamiseks, võib vastutav töötleja teatada, et pärast pädevale järelevalveasutusele rikkumise teatamist on vastutav töötleja saanud nõu rikkumisega tegelemiseks ja selle mõju vähendamiseks. Vastutav töötleja peaks vajadusel samuti andma üksikisikutele konkreetseid soovitusi, et nad saaksid end kaitsta rikkumise võimalike kahjulike tagajärgede eest, näiteks määrama uue salasõna, kui juurdepääsuvolituste kaitstust on rikutud. Veel kord, vastutav töötleja võib valida, millist teavet ta lisaks siinsele edastab.

C. Üksikisikutega kontakteerumine

[36] Vt ka põhjendus 86.

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

Andmesubjekte tuleks rikkumisest teavitada erisõnumite abil ning neid ei tohiks edastada koos muu teabega, näiteks uuendustega, uudiskirjadega või tavasõnumitega. See aitab rikkumisest teavitamise muuta selgeks ja läbipaistvaks.

Läbipaistva suhtlemisviiside näidete hulgas on otseedastus (nt e-post, SMS, otsesõnum), silmapaistvad bännerid või teated veebisaidil, otsepostitus ja silmapaistvad reklaamid tükimeedias. Üksnes pressiteates või korporatiivses blogis esitatud teade ei ole tõhus viis, kuidas üksikisikuid rikkumisest teavitada. Artikli 29 töörühm soovitab vastutavatel töötlejatel valida vahend, mille puhul on tõenäosus, et teave jõuab nõuetekohaselt kõikide mõjutatud üksikisikuteni, võimalikult suur. Olenevalt olukorrast võib see tähendada, et vastutav töötleja kasutab ühe suhtluskanali asemel mitut suhtluskanalit.

Vastutavatel töötlejatel võib tekkida vajadus tagada, et suhtlus on ligipääsetav sobivates alternatiivvormingutes ja asjaomastes keeltes tagamaks, et üksikisikud saavad aru neile edastatud teabest. Näiteks sobib üksikisikute teavitamiseks rikkumisest üldiselt keel, mida kasutatakse tavapärases ärisuhtluses teabe saajaga. 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 ressurse. Peamine on aidata andmesubjektidel mõista rikkumise laadi ja samme, mida nad saavad enda kaitseks astuda.

Vastutavad töötlejad saavad kõige paremini teha kindlaks üksikisikute teavitamiseks sobiva suhtluskanali, eelkõige juhul, kui klientidega suheldakse sageli. Siiski on ilmselge, et vastutav töötleja peab olema ettevaatlik rikutud suhtluskanali kasutamisel, kuna seda võivad kasutada ka vastutava töötleja nime all esinevad ründajad.

Samas on 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.“

Vastutavad töötlejad võivad seetõttu soovida kontakteeruda ja pidada nõu järelevalveasutusega, et saada abi mitte ainult seoses andmesubjektidele rikkumisest teatamisega kooskõlas artikliga 34, vaid ka seoses üksikisikutele saadetavate sobivate teadetega ja sobivaima kontakteerumisviisiga.

Sellega on seotud 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 rikkumisest teavitamisega mõjutatud isikutele seni, kuni see ei takista uurimist. Andmesubjekte tuleb pärast sellist viivitust siiski kohe teavitada.

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

D. Tingimused, mille puhul teavitamine ei ole vajalik

Artikli 34 lõikes 3 on esitatud kolm tingimust, mille täitmise korral ei ole vaja rikkumisest üksikisikuid teavitada. Need on:

- Vastutav töötleja on kohaldanud nõuetekohaseid tehnilisi ja organisatoorseid meetmeid isikuandmete kaitsmiseks enne rikkumist, eelkõige neid meetmeid, mis muudavad isikuandmed loetamatuks kõigile, kellel puuduvad volitused andmetele juurdepääsuks. See võib hõlmata näiteks isikuandmete kaitsmist uusima krüpteeringu või sõnestuse abil.
- Kohe pärast rikkumist on vastutav töötleja astunud samme tagamaks, et üksikisikute õigusi ja vabadusi ähvardav suur oht tõenäoliselt enam ei realiseeru. Näiteks, olenevalt olukorrast, võis vastutav töötleja suuta kohe kindlaks teha isikuandmete juurde pääsenud isiku ja võtta tema vastu meetmed enne, kui ta sai nende andmetega midagi ette võtta. Endiselt tuleb analüüsida konfidentsiaalsusega seotud rikkumise võimalikke tagajärgi ja jällegi teha seda olenevalt asjaomaste andmete laadist.
- Üksikisikutega kontakteerumine nõuab ebaproportsionaalseid jõupingutusi[37] näiteks siis, kui nende kontaktandmed on rikkumise tõttu kadunud või neid ei teatud kohe alguses. Näiteks on statistikabüroo ladu üle ujutatud ja isikuandmeid sisaldavad dokumendid talletati ainult paberkujul. Vastutav töötleja peab tegema avaliku teate või võtma sarnase meetme, mille abil üksikisikuid teavitatakse ühtemoodi tõhusal viisil. Ebaproportsionaalse jõupingutuse vältimiseks võib näha ette tehnilise korra, et teha rikkumisega seotud teave selle taotlejatele kättesaadavaks – sellest võib abi olla rikkumise tõttu mõjutatud üksikisikutel, kellega vastutav töötleja ei saa muul viisil kontakteeruda.

Vastutavad töötlejad peaksid kooskõlas vastutamise põhimõttega näitama järelevalveasutusele, et nad täidavad ühte või rohkem kui ühte tingimust [38]. Tuleb meeles pidada, et kuna alguses puudub vajadus teavitada, sest tõenäolist ohtu füüsiliste isikute õigustele ja vabadustele ei ole, võib see aja jooksul muutuda ning ohu suurust tuleb uuesti hinnata.

Kui vastutav töötleja otsustab üksikisikuid rikkumisest mitte teavitada, on artikli 34 lõikes 4 selgitatud, et järelevalveasutus võib seda nõuda, kui ta leiab, et rikkumine kujutab endast üksikisikutele tõenäoliselt suurt ohtu. Või leiab järelevalveasutus, et 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 oma volituste ja karistuste kohaldamist.

IV. **Ohu ja suure ohu hindamine**

A. Oht teavitamise käivitajana

Ehkki isikuandmete kaitse üldmääruses on kehtestatud kohustus teavitada, ei kehti see nõue kõikides olukordades:

- Pädeva järelevalveasutuse teavitamine on vajalik, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele.

[37] Vt artikli 29 töörühma suuniseid läbipaistvuse kohta, kus käsitletakse ebaproportsionaalsete jõupingutuste küsimust, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Vt artikli 5 lõige 2

- Üksikisikule teatatakse rikkumisest üksnes siis, kui rikkumisest tuleneb tõenäoliselt suur oht nende õigustele ja vabadustele.

See tähendab, et vahetult pärast rikkumisest teada saamist on väga oluline, et vastutav töötleja peaks püüdma lisaks intsidendi ulatuse piiramisele hindama samuti sellest tulenevat ohtu. Selleks on kaks olulist põhjust: esiteks, teades üksikisikule avalduva mõju tõenäosust ja võimalikku tõsidust, on vastutaval töötlejal lihtsam astuda tõhusaid samme rikkumise ulatuse piiramiseks ja sellega tegelemiseks; teiseks, see aitab kindlaks määrata, kas järelevalveasutuse ja asjaomaste üksikisikute teavitamine on vajalik.

Nagu eespool sai selgitatud, rikkumisest teatamine on vajalik, välja arvatud juhul, kui rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele, ning peamine põhjus andmesubjektide teavitamiseks on see, kui rikkumisest tuleneb *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 ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning süüteoasjades süüdimõistvate kohtuotsuste ja süütegude ning nendega seotud turvameetmete kohta, tuleks sellise kahju esinemist pidada tõenäoliseks[39].

B. Tegurid, mida kaaluda ohu hindamisel

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

Tuleb märkida, et inimeste õigustele ja vabadustele rikkumisest tuleneva ohu hindamise kese on erinev kui andmekaitsealase mõjuhinnangu[40] käigus hinnatava ohu puhul. Andmekaitsealase mõjuhinnangu käigus kaalutakse nii plaanipäraselt toimuva andmetöötluse ohte kui ka rikkumisest tulenevaid ohte. Võimaliku rikkumise analüüsimisel vaadeldakse üldiselt rikkumise esinemise tõenäosust ja võimalikku andmesubjektile tulenevat kahju; teisisõnu, hinnatakse hüpoteetilist sündmust. Tegeliku rikkumise puhul on sündmus juba toimunud ja tähelepanu on täielikult suunatud rikkumisest tuleneva ohu mõjule, mis avaldub üksikisikule.

Näide

Andmekaitsealases mõjuhinnangus soovitatakse, et isikuandmete kaitsmiseks mõeldud turvatarkvara kasutamine on sobiv meede, et tagada sellisele ohule vastav turvalisuse tase, mida andmete töötlemine võiks muul viisil avaldada üksikisikutele. Kuid, kui seejärel avastatakse turvaauk, muudab see tarkvara suutlikkust piirata kaitstavatele isikuandmetele avalduvat ohtu ja seega tuleb käimasoleva andmekaitsealase mõjuhinnangu käigus tarkvara uuesti hinnata.

Tarkvara turvaauk kasutatakse hiljem ära ja toimub rikkumine. Vastutav töötleja peaks hindama rikkumise spetsiifilisi tingimusi, mõjutatud andmeid ning võimalikku mõju üksikisikutele ning samuti seda, kuidas oht tõenäoliselt materialiseerub.

[39] Vaata põhjendused 75 ja 85.

[40] Vaata töörühma suunised andmekaitsealase mõjuhinnangu kohta: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Sellest tulenevalt peaks vastutav töötleja rikkumisest tuleneva ja üksikisikutele avalduva ohu hindamisel arvestama rikkumise spetsiifiliste tingimustega, sealhulgas võimaliku mõju tõsidust ja selle avaldumise tõenäosust. Artikli 29 töörühm seetõttu soovitab, et hindamisel tuleks võtta arvesse järgmisi kriteeriume[41]:

- Rikkumise liik

Toimunud rikkumise liik võib mõjutada üksikisikutele avalduva ohu suurust. Näiteks võib konfidentsiaalsusega seotud rikkumisel, mille käigus avaldatakse 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

Kahtlemata on ohu hindamisel väga oluline rikutud isikuandmete liik ja tundlikkus.Tavaliselt, mida tundlikumad andmed, seda suurem on oht kahju tekkimiseks asjaomastele isikutele, kuid tähelepanu tuleb pöörata ka teistele isikuandmetele, mis andmesubjekti kohta võivad juba olla kättesaadavad. Näiteks ei ole tõenäoline, et üksikisiku nime ja aadressi avaldamine tavalises olukorras põhjustaks olulist kahju. Kuid, kui lapsendanud vanema nimi ja aadress avaldatakse sünnivanematele, võivad tagajärjed olla väga tõsised nii lapsendanud vanema kui ka lapse jaoks.

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

Osa isikuandmete liike võivad esialgu näida suhteliselt süütutena, kuid siiski tuleb hoolikalt analüüsida, mida need andmed võivad avaldada asjaomase üksikisiku kohta. Korrapäraselt saadetisi saavate klientide nimekiri ei pruugi olla väga tundlik, kuid samad andmed klientide kohta, kes on palunud puhkuse tõttu peatada saadetiste edastamise, võivad osutuda kasulikuks teabeks kurjategijatele.

Samamoodi võib väike hulk väga tundlikke isikuandmeid avaldada suurt mõju üksikisikule ning suur hulk üksikasju võib avaldada palju rohkem teavet asjaomase üksikisiku kohta. Samuti võib rikkumine, mis mõjutab paljude andmesubjektide isikuandmete suuri mahtusid, avaldada mõju samaväärselt suurele üksikisikute arvule.

- Üksikisikute kindlaks määramise lihtsus

Oluline on analüüsida, kui lihtne on osapoolel, kellel on juurdepääs rikutud kaitstusega isikuandmetele, määrata kindlaks konkreetseid üksikisikuid või sobitada üksikisikute kindlaks tegemiseks nende andmed muu teabega. Olenevalt olukorrast võib identifitseerimine olla võimalik vahetult rikutud isikuandmete alusel ilma spetsiaalse uurimistööta üksikisiku identiteedi leidmiseks või võib isikuandmete sobitamine konkreetse üksikisikuga olla äärmiselt raske, kuid teatavate tingimuste esinemisel võib see siiski võimalik olla. Identifitseerimine rikutud andmete alusel võib olla võimalik vahetult, kuid see võib samuti sõltuda rikkumise konkreetsetest asjaoludest ning asjaomaste isikuandmete üksikasjade avalikust kättesaadavusest. See võib olla asjakohasem konfidentsiaalsusega ja kättesaadavusega seotud rikkumiste puhul.

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

Nagu eespool öeldud, nõuetekohase krüpteeringutasemega kaitstud isikuandmed muutuvad loetamatuks volitamata isikutele, kellel puudub krüpteerimisvõti. Lisaks võib vähendada rikkumise esinemisel üksikisikute tuvastamise tõenäosust pseudonümiseerimine (määratletud artikli 4 lõikes 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 viisiks, mis muudab andmed loetamatuks.

- Tagajärgede tõsidus üksikisikute jaoks.

Olenevalt rikkumisega seotud isikuandmete laadist, näiteks andmete erikategooriad, võib võimalik oht üksikisikutele olla eriti suur, eelkõige juhul, kui rikkumise tagajärjeks võib olla identiteedivargus või -pettus, tervisekahjustus, psühholoogilised kannatused, alandamine või maine kahjustamine. Kui rikkumine puudutab haavatavate üksikisikute isikuandmeid, võivad nad sattuda suuremasse ohtu.

See, kas vastutav töötleja teab, et isikuandmed on selliste inimeste käes, 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 lõikes 10 määratletud kolmandale isikule või teisele teabe saajale. See võib juhtuda näiteks siis, kui isikuandmed saadetakse ekslikult organisatsiooni valesse osakonda või sageli kasutatava tarnija organisatsioonile. Vastutav töötleja võib esitada teabe saajale taotluse saadud andmed kas tagastada või turvaliselt hävitada. Mõlemal juhul ja arvestades, et vastutaval töötlejal on nendega püsiv suhe ja ta on teadlik nende menetlustest, varasemast tegevusest ja muudest asjaomastest üksikasjadest, võib andmete saajat pidada usaldusväärseks. Teisisõnu, vastutaval töötlejal võib olla teatav kindlus seoses andmete saajaga, et ta võib põhjendatult loota, et see isik ei loe ega kasuta talle ekslikult saadetud andmeid ning täidab talle andmete tagasisaatmise juhiseid. Isegi, kui andmeid on kasutatud, võib vastutav töötleja endiselt olla kindel, et andmete saaja ei võta andmetega midagi ette ning tagastab need vastutavale töötlejale kohe ning teeb andmete taastamisel koostööd. Sellistel juhtudel võib vastutav töötleja lülitada rikkumisjärgsesse ohuhinnangusse järgmise asjaolu – andmete vastuvõtja on usaldusväärne ja see võib vähendada rikkumise tagajärgede tõsidust, kuid see ei tähenda, et rikkumist ei toimunud. Kuid see võib siiski omakorda kõrvaldada üksikisikutele avalduva ohu tõenäosuse, seega ei ole vaja teavitada järelevalveasutust või mõjutatud üksikisikuid. Jällegi sõltub see igast üksikust juhtumist eraldi. Sellele vaatamata peab vastutav töötleja endiselt säilitama teabe rikkumise kohta osana tema üldisest kohustusest säilitada rikkumise andmed (vt allpool V jagu).

Samuti tuleb pöörata tähelepanu üksikisikutele tekkivate tagajärgede kestusele, mille puhul võib mõju vaadelda suuremana, kui selle mõju on pikaajaline.

- Üksikisikute eriomadused

Rikkumine võib mõjutada laste või teiste haavatavate üksikisikute isikuandmeid ja seada nad seetõttu suuremasse ohtu. Üksikisikute puhul võivad esineda ka teised tegurid, mis võivad nende jaoks mõjutada rikkumise mõju suurust.

- Vastutava töötleja eriomadused

Vastutava töötleja roll ja tema tegevuse laad võivad üksikisikute jaoks mõjutada rikkumisest tuleneva ohu suurust. Näiteks töötlevad meditsiiniasutused isikuandmete erikategooriaid ehk võrreldes ajalehe meililisti andmetega, avaldub üksikisikutele isikuandmete rikkumisel suurem oht.

- Mõjutatud üksikisikute arv

Rikkumine võib mõjutada vaid ühte või mõnda üksikisikut või mitut tuhandet ja rohkemaid. Üldiselt, mida suurem on mõjutatud üksikisikute arv, seda suuremat mõju võib rikkumine avaldada. Rikkumine

võib siiski tõsiselt mõjutada kasvõi ühte üksikisikut, olenevalt isikuandmete laadist ning kontekstist, kus selle kaitstus rikuti. Jällegi, peamine on analüüsida mõju tõenäosust ja tõsidust asjaomastele isikute jaoks.

- Üldised tegurid

Kui hinnatakse rikkumisest tulenevat võimalikku ohtu, peab vastutav töötleja seetõttu analüüsima korraga üksikisikute õigustele ja vabadustele avalduva võimaliku mõju tõsidust ja selle esinemise tõenäosust. On selge, et kui rikkumise tagajärjed on tõsisemad, on oht suurem ja samamoodi, kui nende esinemise tõenäosus on suurem, on ohu suurus samuti kõrgem. Kahtluse korral tuleks vastutaval töötlejal olla pigem ettevaatlik ja rikkumisest teatada. Lisas B esitatakse mitmeid kasulikke näiteid erinevate rikkumiste kohta, mis avaldavad üksikisikutele ohtu või suurt ohtu.

Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA) on koostanud soovitused rikkumise tõsiduse hindamise metoodika kohta – kasulik materjal vastutavatele töötlejatele ja volitatud töötlejatele rikkumise lahendamise juhtimise kava[42] koostamisel.

V. Vastutus ja dokumenteerimine

A. Rikkumiste dokumenteerimine

Vaatamata sellele, kas rikkumisest tuleb järelevalveasutust teavitada, peab vastutav töötleja dokumenteerima kõik rikkumised, nagu 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.“

See on seotud isikuandmete kaitse üldmääruse artikli 5 lõikes 2 sätestatud vastutamise põhimõttega. Teavitamisele mittekuuluvate ja ka teavitamisele kuuluvate rikkumiste registreerimise eesmärk on samuti seotud vastutava töötleja artikli 24 kohaste kohustustega ning järelevalveasutus võib asjaomaseid dokumente näha küsida. Seetõttu julgustatakse vastutavaid töötlejaid looma asutusesisest rikkumiste registrit vaatamata sellele, kas teavitamine on neile kohustuslik või mitte[43].

Ehkki vastutav töötleja otsustab, millist meetodit ja struktuuri rikkumiste dokumenteerimisel kasutada, peab dokumenteeritavas teabes olema iga juhtumi kohta kirjas alati põhiandmed. Nagu nõutud artikli 33 lõikes 5, peab vastutav töötleja dokumenteerima rikkumisega seotud üksikasjad, mis peaks hõlmama rikkumise põhjusi, toimunut ja mõjutatud isikuandmed. Samuti peaks see hõlmama rikkumise mõju ja tagajärgi ning vastutava töötleja poolt võetud parandusmeetmeid.

Isikuandmete kaitse üldmääruses ei ole selliste dokumentide säilitamise ajavahemikku. Kui sellised dokumendid sisaldavad isikuandmeid, on vastutaval töötlejal kohustus määrata kindlaks dokumentide säilitamise sobiv ajavahemik vastavalt isikuandmete töötlemisega seotud põhimõtetele[44] ja täita

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

[43] Vastutav töötleja võib otsustada dokumenteerida rikkumised osana töötlemistegevuste dokumenteerimisest, mida tehakse vastavalt artiklile 30. Eraldi registrit ei ole vaja, kui rikkumisega seotud teave on selgelt tuvastatav ja registrist saab taotluse korral teha rikkumisega seotud andmete väljavõtte.

[44] Vt artikkel 5.

töötlemise õiguslikke tingimusi[45]. Vastutaval töötlejal on artikli 33 lõikest 5 tulenev kohustus dokumentatsioon säilitada, kuna järelevalveasutus võib nõuda tõendite esitamist selles artiklis sätestatud nõuete või üldisemalt vastutamise põhimõtte täitmise kohta. Selge on see, et kui dokumendid ei sisalda isikuandmeid, ei kohaldata isikuandmete kaitse üldmääruse kohast piirangu põhimõtet[46].

Lisaks nendele üksikasjadele soovitab artikli 29 töörühm, et vastutav töötleja dokumenteeriks samuti rikkumisele reageerimiseks tehtud otsuste põhjendused. Eelkõige tuleks asjaomane ostus dokumenteerida siis, kui rikkumisest ei teatata. See peaks sisaldama põhjuseid, miks vastutav töötleja leiab, et rikkumisest ei tulene ohtu üksikisikute õigustele ja vabadustele[47]. Alternatiivina, kui vastutav töötleja leiab, et artikli 34 lõike 3 tingimused on täidetud, peaks ta olema suuteline esitama piisavaid tõendeid selle kinnituseks.

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

Kui vastutav töötleja teatab rikkumisest mõjutatud üksikisikutele, peaks ta seda tegema läbipaistval viisil ning suhtlemine peaks olema tõhus ja õigeaegne. Sellest tulenevalt võiks vastutav töötleja siinkohal üles näidata vastutustunnet ja kuulekust ning säilitada tõendid sellise suhtlemise kohta.

Artiklite 33 ja 34 nõuete paremaks täitmiseks oleks hea, kui nii vastutav töötleja kui ka volitatud töötleja on kehtestanud dokumenteeritud teatamismenetluse, millega kehtestatakse kord, mida järgida pärast rikkumise avastamist, sealhulgas kuidas intsidendi ulatust piirata, juhtida ja esialgset olukorda taastada ning samuti kuidas ohtu hinnata ja rikkumisest teatada. Isikuandmete kaitse üldmääruse järgimise demonstreerimiseks võib samuti olla kasulik näidata, et töötajaid on teavitatud selliste menetluste ja mehhanismide olemasolust ning nad teavad, kuidas rikkumise korral toimida.

Tuleb märkida, et kui rikkumine jäetakse nõuetekohaselt dokumenteerimata, võib järelevalveasutus kasutada oma artikli 58 kohaseid volitusi või määrata kooskõlas artikliga 83 haldustrahvi.

B. Andmekaitseametniku roll

Vastutav töötleja või volitatud töötleja võib määrata andmekaitseametniku[48] artikli 37 nõude järgi 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.

Rikkumisest teavitamise 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 artiklil 33 lõike 3 punkti b kohaselt edastama oma andmekaitseametniku või muu kontaktisiku nime ja kontaktandmed.

---

[45] Vt artikkel 6 ja samuti artikkel 9.

[46] Vt artikli 5 lõike 1 punkt e.

[47] Vt põhjendus 85

[48] Vt töörühma suunised andmekaitseametnike kohta: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

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

Need asjaolud tähendavad, et andmekaitseametnikul peaks olema otsustav roll nii rikkumiste ennetamisel ja nendeks valmistumisel, nõustades ja nõuetele vastavust kontrollides, aga ka rikkumise ajal (st järelevalveasutuse teavitamisel) ja sellele järgneva uurimise ajal, mida korraldab järelevalveasutus. Seda arvestades soovitab artikli 29 töörühm, et andmekaitseametnikku teavitatakse rikkumisest kohe ja ta kaasatakse rikkumise juhtimise ja sellest teavitamise menetlusse algusest lõpuni.

VI. Teiste õigusaktide kohased teavitamise kohustused

Lisaks isikuandmete kaitse üldmääruse alusel toimuvale teavitamisele ja suhtlemisele ning üldmäärusest sõltumatult peaksid vastutavad töötlejad olema samuti teadlikud turvaintsidentidest teatamise nõuetest, mis tulenevad teistest õigusaktidest, mida võidakse nende suhtes kohaldada, ning sellest, kas seetõttu tuleb neil isikuandmetega seotud rikkumisest teavitada samal ajal järelevalveasutust. Sellised nõuded võivad liikmesriigiti erineda; teistes õigusaktides esinevate rikkumisest teatamise nõuete näidete hulgast leiab järgmised õigusaktid ja nende nõuete seose isikuandmete kaitse üldmäärusega:

- Määrus (EL) 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDAS määrus)[49].

eIDAS määruse artikli 19 lõikes 2 on nõutud, et usaldusteenuse osutajad teavitavad järelevalveasutust igast turvarikkumisest või tervikluse kaotsiminekust, millel on märkimisväärne mõju osutatavale usaldusteenusele või selles sisalduvatele isikuandmetele. Kui see on kohaldatav – st kui selline rikkumine või kaotsiminek 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)[50].

Küberturvalisuse direktiivi artiklites 14 ja 16 nõutakse, et oluliste teenuste operaatorid ja digitaalse teenuste osutajad teataksid turvaintsidentidest oma pädevatele asutustele. Nagu küberturvalisuse direktiivi põhjenduses 63[51] tunnistatakse, on intsidendi tagajärjeks sageli isikuandmete kaitstuse rikkumine. Ehkki küberturvalisuse direktiivis nõutakse, et pädevad asutused ja järelevalveasutused teeks koostööd ja vahetaks asjaomast teavet, tuleb olukorras, kus sellised intsidendid on isikuandmetega seotud rikkumised või on selleks muutumas isikuandmete kaitse üldmääruse tähenduses, tuleb asjaomastel operaatoritel ja/või teenuste osutajatel teavitada järelevalveasutust eraldi küberturvalisuse direktiivis kehtestatud intsidendist teatamise nõudest.

Näide

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

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

51 Põhjendus 63: *„Sageli on intsidendi tagajärjeks isikuandmete kaitstuse 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.“*

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

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

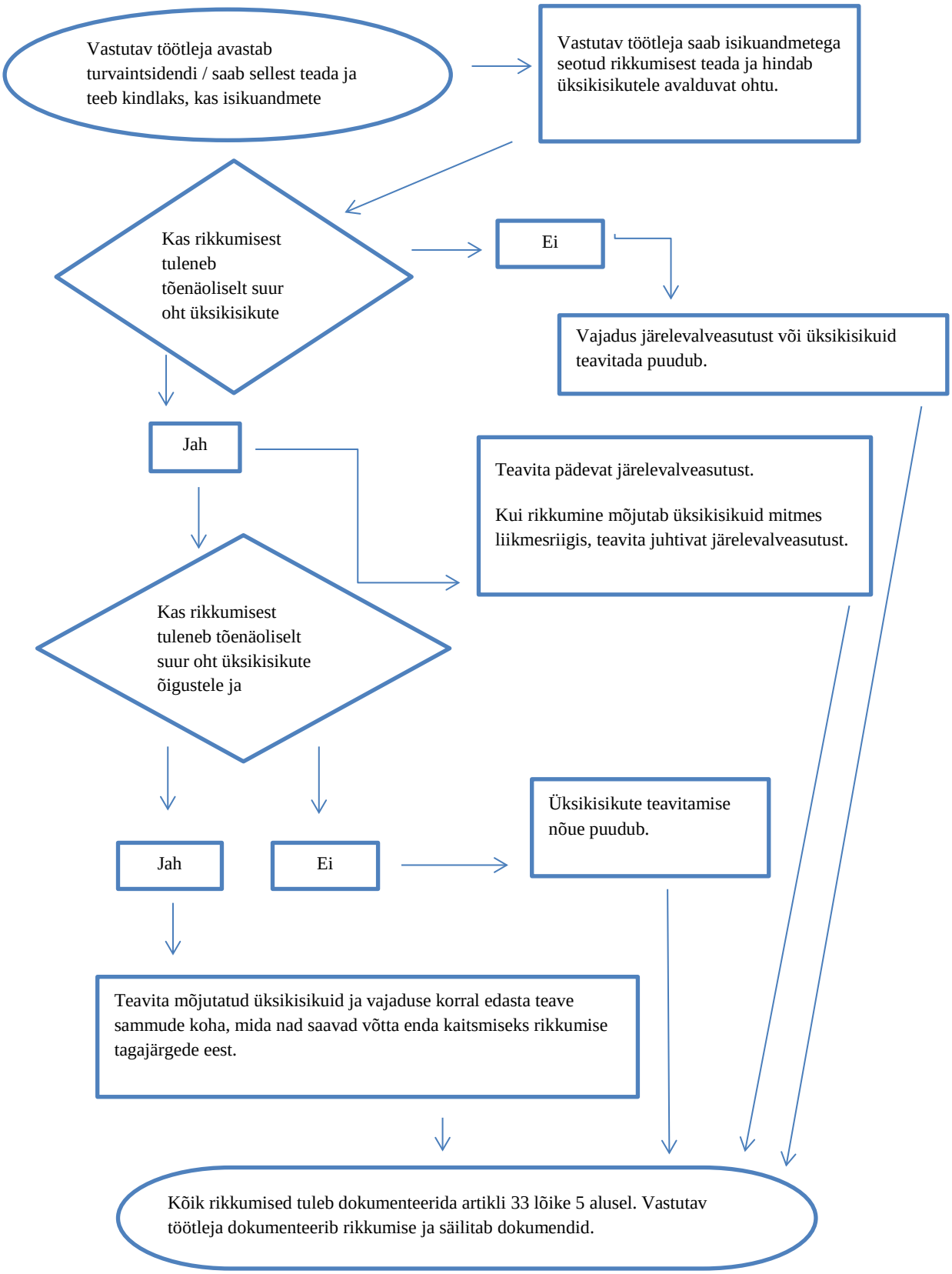
Üldkasutatavate elektrooniliste sideteenuste osutaja direktiivi 2002/58/EÜ[52] kontekstis peab rikkumisest teavitama pädevaid riiklikke asutusi.

Vastutavad töötlejad peaksid samuti olema teadlikud täiendavatest õiguslikest, meditsiinilistest või erialastest teatamiskohustustest, mida kohaldatakse muu korra alusel.

[52] 10. jaanuaril 2017 esitas Euroopa Komisjon privaatsust ja elektroonilist sidet käsitleva määruse ettepaneku, mis asendab direktiivi 2009/136/EÜ ja jätab välja rikkumisest teatamise nõuded. Kuid ettepaneku heakskiitmiseni Euroopa Parlamendis on rikkumisest teatamise nõue kehtiv, vt https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Lisa**

A. Vooskeem rikkumisest teatamise nõuete kohta



B. Näited isikuandmetega seotud rikkumise ja selle kohta, keda teavitada

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. Võti varastati sissemurdmise ajal.	Ei	Ei	Seni, kuni andmed on krüpteeritud uusima algoritmi alusel, andmete varukoopiad on olemas ja unikaalse võtme kaitstust ei ole rikutud ning andmeid saab mõistliku aja jooksul taastada, ei pruugi tegemist olla teavitamist vajava rikkumisega. Kuid, kui selle kaitstus hiljem rikutakse, on teavitamine vajalik.
ii. Vastutav töötleja osutab internetipõhist teenust. Selle teenuse vastu suunatud küberrünnaku tõttu lekivad üksikisikute isikuandmed. Vastutaval töötlejal on kliendid ühes liikmesriigis.	Jah, teavita järelevalveametit, kui tekivad tõenäolised tagajärjed üksikisikute jaoks.	Jah, teavita üksikisikuid olenevalt mõjutatud isikuandmete laadist ja kui tõenäolised tagajärjed üksikisikute jaoks on tõsised.	
iii. Põgus mõneminutiline elektrikatkestus vastutava töötleja kõnekeskuses tähendab, et kliendid ei saa vastutavale töötlejale helistada ja pääseda juurde oma andmetele.	Ei	Ei	Sellest rikkumisest ei pea teatama, kuid see on artikli 33 lõike 5 kohaselt dokumenteerimisele kuuluv intsident. Vastutav töötleja säilitab asjaomased andmed.
iv. Vastutaval töötlejal esineb lunavara rünnak, mille tõttu kõik andmed krüpteeritakse. Varukoopiad ei ole kättesaadavad ja	Jah, teavita järelevalveametit, kui esinevad tõenäolised tagajärjed üksikisikute jaoks, kuna tegemist on kättesaadavuse	Jah, teavita üksikisikuid, olenevalt mõjutatud isikuandmete laadist ja andmete kättesaadavuse puudumise	Kui varukoopia on kättesaadav ja andmed saab taastada õigeaegselt, ei tule sellest järelevalveasutust ja üksikisikuid teavitada, kuna kättesaadavuse ja

andmeid ei saa taastada. Uurimise käigus selgub, et lunavara ainus ülesanne oli andmed krüpteerida ja süsteemis muud pahavara ei olnud.	kaotsiminekuga.	võimalikust mõjust ning muudest võimalikest tagajärgedest.	konfidentsiaalsuse kaotsiminek oli ajutine. Kui järelevalveasutus saab siiski teiste kanalite kaudu intsidendist teada, võib ta kaaluda uurimise läbiviimist, et hinnata artikli 32 turvanõuete järgimist laiemalt.
v. Üksikisik helistab panga kõnekeskusesse ja teatab andmete rikkumisest. Üksikisik on saanud kellegi teise igakuise pangaväljavõtte. Vastutav töötleja korraldab lühikese uurimise (st viib selle 24 tunni jooksul lõpule) ja teeb piisava kindlusega kindlaks, et toimunud on isikuandmetega seotud rikkumine ja kas sellel on süsteemne viga, mis võib tähendada, et mõjutatud 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 lisasamme teiste üksikisikute teavitamiseks, kui nende suhtes esineb suur oht.
vi. Vastutav töötleja peab internetipõhist kauplemiskohta ja tal on kliente mitmes liikmesriigis. Kauplemiskohta küberrünnatakse ning ründaja avaldab veebis kasutajanimed, salasõnad ja varasemate ostude nimekirjad.	Jah, teata 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 peab samuti kaaluma kõiki teisi teavitamise kohustusi, nt digitaalse teenuse osutajana küberturvalisuse direktiivi alusel.
vii. Veebimajutust pakkuv ettevõte, mis tegutseb andmete töötlejana, leiab vea koodis, mis kontrollib	Andmete töötlejana peab veebimajutaja viivitamata teavitama mõjutatud kliente (vastutavaid	Kui üksikisikute suhtes suurt ohtu tõenäoliselt ei esine, ei pea neid teavitama.	Veebimajutaja (volitatud töötleja) peab kaaluma kõiki teisi teavitamise kohustusi (nt digitaalse teenuse pakkujana

kasutajate autoriseerimist. Vea mõjul on võimalik kõikidel kasutajatel pääseda juurde teiste kasutajate kontode üksikasjadele.	töötlejaid). Oletades, et veebimajutaja on korraldanud ettevõttes uurimise, võivad mõjutatud vastutavad töötlejad olla üsnagi kindlad selles osas, kas keegi neist on saanud rikkumise tõttu kahju, ja kas seetõttu saab öelda, et nad „said sellest teada“, kui veebimajutaja (volitatud töötleja) neid teavitas. Vastutav töötleja peab seejärel teavitama järelevalveasutust.		küberturvalisuse direktiivi alusel). Kui puuduvad tõendid selle kohta, et turvaauku kasutatakse vastutavate töötlejate juures, ei pruugi see olla teavitamisele kuuluv rikkumine, kuid tõenäoliselt tuleb see dokumenteerida või on tegemist artikli 32 nõuete täitmatajätmisega.
viii. Küberrünnaku tõttu ei ole tervisekaardid haiglas 30 tunni jooksul kättesaadavad.	Jah, haiglal on kohustus teatada, kuna võib esineda suur oht patsientide heaolule ja privaatsusele.	Jah, teavita mõjutatud üksikisikuid.	
ix. Suure hulga üliõpilaste isikuandmed saadeti ekslikult valesse meililisti, millel on üle 1000 saaja.	Jah, teavita järelevalveasutust.	Jah, teavita üksikisikuid olenevalt asjaomaste isikuandmete ulatusest ja liigist ning võimalike tagajärgede tõsidusest.	
x. Otseturunduse meil edastatakse saajatele „adressaat:“ või „koopia:“ realt, võimaldades seega igal saajal näha teiste saajate meiliaadresse.	Jah, järelevalveasutuse teavitamine võib olla kohustuslik, kui rikkumine mõjutab paljusid üksikisikuid, kui avaldatakse tundlikke andmeid (nt psühhoterapeudi meililist) või kui teised asjaolud kujutavad endast suurt ohtu (nt meilis on märgitud algsed salasõnad).	Jah, teavita üksikisikuid olenevalt asjaomaste isikuandmete ulatusest ja liigist ning võimalike tagajärgede tõsidusest.	Teatamine ei pruugi olla vajalik, kui tundlikke andmeid ei avaldata, ja kui avaldatakse vaid üksikud meiliaadressid.