Suunised

Suunised 01/2021

isikuandmetega seotud rikkumisest teatamise näidete kohta

Vastu võetud 14. detsembril 2021

Versioon 2.0

Versioonid

Versioon 2.0	14.12.2021	Suuniste vastuvõtmine pärast avalikku konsultatsiooni
Versioon 1.0	14.1.2021	Suuniste vastuvõtmine avalikuks konsultatsiooniks

Sisukord

1 SISSEJUHATUS 5

2 LUNAVARA 8

2.1 JUHTUM nr 1. Lunavara nõuetekohaselt varundatud andmete korral ja ilma andmelekketa 8

2.1.1 JUHTUM nr 1. Eelnevad meetmed ja riskihindamine 8

2.1.2 JUHTUM nr 1. Leevendamine ja kohustused 9

2.2 JUHTUM nr 2. Lunavara nõuetekohaselt varundamata andmete korral 10

2.2.1 JUHTUM nr 2. Eelnevad meetmed ja riskihindamine 10

2.2.2 JUHTUM nr 2. Leevendamine ja kohustused 11

2.3 JUHTUM nr 3. Lunavara varundatud andmete korral ja ilma andmelekketa haigla puhul 13

2.3.1 JUHTUM nr 3. Eelnevad meetmed ja riskihindamine 13

2.3.2 JUHTUM nr 3. Leevendamine ja kohustused 13

2.4 JUHTUM nr 4. Lunavara varundamata andmete korral ja koos andmelekkega 14

2.4.1 JUHTUM nr 4. Eelnevad meetmed ja riskihindamine 14

2.4.2 JUHTUM nr 4. Leevendamine ja kohustused 15

2.5 Korralduslikud ja tehnilised meetmed lunavararünnete mõju ennetamiseks/leevendamiseks 15

3 Andmeleket hõlmavad RÜNDED 16

3.1 JUHTUM nr 5. Töökohale kandideerimise taotluste andmete leke veebisaidilt 17

3.1.1 JUHTUM nr 5. Eelnevad meetmed ja riskihindamine 17

3.1.2 JUHTUM nr 5. Leevendamine ja kohustused 17

3.2 JUHTUM nr 6. Veebisaidilt räsitud parooli leke 18

3.2.1 JUHTUM nr 6. Eelnevad meetmed ja riskihindamine 18

3.2.2 JUHTUM nr 6. Leevendamine ja kohustused 18

3.3 JUHTUM nr 7. Kontovargusega seotud rünne panga veebisaidil 19

3.3.1 JUHTUM nr 7. Eelnevad meetmed ja riskihindamine 19

3.3.2 JUHTUM nr 7. Leevendamine ja kohustused 20

3.4 Korralduslikud ja tehnilised meetmed häkkerite rünnete mõju ennetamiseks/leevendamiseks 20

4 ORGANISATSIOONISISESED INIMESTEga seotud RISKIALLIKAD 21

4.1 JUHTUM nr 8. Äriandmete varastamine töötaja poolt 21

4.1.1 JUHTUM nr 8. Eelnevad meetmed ja riskihindamine 21

4.1.2 JUHTUM nr 8. Leevendamine ja kohustused 22

4.2 JUHTUM nr 9. Andmete juhuslik edastamine usaldusväärsele kolmandale isikule 23

4.2.1 JUHTUM nr 9. Eelnevad meetmed ja riskihindamine 23

4.2.2 JUHTUM nr 9. Leevendamine ja kohustused 23

4.3 Korralduslikud ja tehnilised meetmed inimestega seotud organisatsioonisiseste riskiallikate mõju ennetamiseks/leevendamiseks 23
5 KAOTATUD VÕI VARASTATUD SEADMED JA PABERKANDJAL DOKUMENDID 24
5.1 JUHTUM nr 10. Varastatud materjal, kuhu on salvestatud krüpteeritud isikuandmed 25
5.1.1 JUHTUM nr 10. Eelnevad meetmed ja riskihindamine 25
5.1.2 JUHTUM nr 10. Leevendamine ja kohustused 25
5.2 JUHTUM nr 11. Varastatud materjal, kuhu on salvestatud krüpteerimata isikuandmed 25
5.2.1 JUHTUM nr 11. Eelnevad meetmed ja riskihindamine 26
5.2.2 JUHTUM nr 11. Leevendamine ja kohustused 26
5.3 JUHTUM nr 12. Tundlikke andmeid sisaldavad varastatud paberkandjal failid 26
5.3.1 JUHTUM nr 12. Eelnevad meetmed ja riskihindamine 27
5.3.2 JUHTUM nr 12. Leevendamine ja kohustused 27
5.4 Korralduslikud ja tehnilised meetmed seadmete kaotamise või varguse mõju ennetamiseks/leevendamiseks 27
6 EKSLIK POSTITAMINE 28
6.1 JUHTUM nr 13. Posti teel saadetud kirjaga seotud eksimus 28
6.1.1 JUHTUM nr 13. Eelnevad meetmed ja riskihindamine 28
6.1.2 JUHTUM nr 13. Leevendamine ja kohustused 29
6.2 JUHTUM nr 14. Kirja teel eksikombel saadetud äärmiselt konfidentsiaalsed isikuandmed 29
6.2.1 JUHTUM nr 14. Eelnevad meetmed ja riskihindamine 29
6.2.2 JUHTUM nr 14. Leevendamine ja kohustused 29
6.3 JUHTUM nr 15. Kirja teel eksikombel saadetud isikuandmed 29
6.3.1 JUHTUM nr 15. Eelnevad meetmed ja riskihindamine 30
6.3.2 JUHTUM nr 15. Leevendamine ja kohustused 30
6.4 JUHTUM nr 16. Posti teel saadetud kirjaga seotud eksimus 30
6.4.1 JUHTUM nr 16. Eelnevad meetmed ja riskihindamine 31
6.4.2 JUHTUM nr 16. Leevendamine ja kohustused 31
6.5 Korralduslikud ja tehnilised meetmed eksliku postitamise mõju ennetamiseks/leevendamiseks 31
7 Muud juhtumid – sotsiaalne manipulatsioon 32
7.1 JUHTUM nr 17. Identiteedivargus 32
7.1.1 JUHTUM nr 17. Riskihindamine, leevendamine ja kohustused 32
7.2 JUHTUM nr 18. E-kirjadega seotud andmeleke 33
7.2.1 JUHTUM nr 18. Riskihindamine, leevendamine ja kohustused 33

EUROOPA ANDMEKAITSENÕUKOGU,

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

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse oma töökorra artikleid 12 ja 22,

võttes arvesse komisjoni teatist Euroopa Parlamendile ja nõukogule „Andmekaitse kodanike võimestajana ja ELi valmistumine digiüleminekuks – isikuandmete kaitse üldmääruse kohaldamise kaks esimest aastat“,[2]

ON VASTU VÕTNUD JÄRGMISED SUUNISED.

1 SISSEJUHATUS

1. Isikuandmete kaitse üldmäärusega kehtestatakse nõue teavitada teatavatel juhtudel isikuandmetega seotud rikkumisest pädevat riiklikku järelevalveasutust (edaspidi „järelevalveasutus“) ja teavitada rikkumisest andmesubjekte, kelle isikuandmeid rikkumine mõjutab (artiklid 33 ja 34).

2. Artikli 29 töörühm juba koostas 2017. aasta oktoobris andmetega seotud rikkumisest teatamise kohta *üldised* suunised, milles analüüsitakse isikuandmete kaitse üldmääruse asjaomaseid jagusid („Suunised, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel“) (edaspidi „suunised WP250“)[3]. Oma laadi ja ajastuse tõttu ei käsitletud nendes suunistes aga kõiki praktilisi küsimusi piisavalt üksikasjalikult. Seepärast tekkis vajadus *praktilise suunitlusega juhtumipõhiste* suuniste järele, mis tugineksid järelevalveasutuste kogemustele alates sellest ajast, mil isikuandmete kaitse üldmäärust hakati kohaldama.

3. Käesoleva dokumendiga täiendatakse suuniseid WP250 ja see kajastab EMP riikide järelevalveasutuste ühiseid kogemusi alates ajast, mil isikuandmete kaitse üldmäärust kohaldama hakati. Dokumendi eesmärk on aidata vastutavatel töötlejatel otsustada, kuidas andmetega seotud rikkumisi käsitleda ja milliseid tegureid riskihindamisel kaaluda.

[1] Käesolevas dokumendis esitatud viiteid liikmesriikidele tuleks käsitada viidetena EMP liikmesriikidele.

[2] COM(2020) 264 final, 24. juuni 2020.

[3] Artikli 29 alusel asutatud andmekaitse töörühma 6. veebruari 2018. aasta suunised WP250 rev.1, mis käsitlevad isikuandmetega seotud rikkumisest teatamist määruse 2016/679 alusel (Euroopa Andmekaitsenõukogu poolt heaks kiidetud), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. Selleks et vastutav töötleja ja volitatud töötleja saaksid rikkumist käsitleda, peavad nad selle kõigepealt ära tundma. Isikuandmete kaitse üldmääruse artikli 4 lõikes 12 on „isikuandmetega seotud rikkumine“ määratletud kui „turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu“.

5. Artikli 29 töörühm selgitas oma arvamuses 03/2014 rikkumisest teatamise kohta[4] ja suunistes WP250, et rikkumisi võib jaotada kategooriatesse vastavalt järgmisele kolmele hästi tuntud infoturbe põhimõttele:

   - „konfidentsiaalsusega seotud rikkumine“ – isikuandmete loata või juhuslik avalikustamine või neile juurdepääs;
   - „terviklusega seotud rikkumine“ – isikuandmete loata või juhuslik muutmine;
   - „kättesaadavusega seotud rikkumine“ – isikuandmetele juurdepääsu juhuslik või loata kaotsiminek või hävitamine[5].

6. Rikkumine võib üksikisikuid kahjulikult mõjutada mitmel viisil ja selle tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju. Isikuandmete kaitse üldmääruses on selgitatud, et see võib hõlmata kontrolli kaotamist oma isikuandmete üle või õiguste piiramist, diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, pseudonümiseerimise loata tühistamist, maine kahjustamist ja ametisaladusega kaitstud andmete konfidentsiaalsuse kadu. Samuti võib see hõlmata muud tõsist majanduslikku või sotsiaalset kahju asjaomastele isikutele. Üks vastutava töötleja kõige olulisem kohustus on hinnata neid riske andmesubjektide õigustele ja vabadustele ning võtta sobilikke tehnilisi ja korralduslikke meetmeid selliste riskide kõrvaldamiseks.

7. Sellest tulenevalt peab vastutav töötleja isikuandmete kaitse üldmääruse kohaselt

   - dokumenteerima kõik isikuandmetega seotud rikkumised, sealhulgas isikuandmetega seotud rikkumise asjaolud, selle mõju ja võetud parandusmeetmed[6];
   - teatama isikuandmetega seotud rikkumisest järelevalveasutusele, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele[7];
   - teavitama andmesubjekti isikuandmetega seotud rikkumisest, kui isikuandmetega seotud rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele[8].

8. Andmetega seotud rikkumised on iseenesest probleemid, kuid samuti võivad need osutada haavatavale – ja võimalik, et aegunud – andmeturbekorrale ning kõrvaldamist vajavatele süsteemi puudustele. Üldreeglina on alati parem andmetega seotud rikkumisi nendeks eelnevalt valmistudes vältida, sest paljud

---

[4] Artikli 29 alusel asutatud andmekaitse töörühma 25. märtsi 2014. aasta arvamus 03/2014 isikuandmetega seotud rikkumistest teatamise kohta (WP213), lk 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Vt suunised WP250, lk 7. Tuleb arvestada, et andmetega seotud rikkumine võib puudutada üht kategooriat või samaaegselt või seotult mitut kategooriat.

[6] Isikuandmete kaitse üldmääruse artikli 33 lõige 5.

[7] Isikuandmete kaitse üldmääruse artikli 33 lõige 1.

[8] Isikuandmete kaitse üldmääruse artikli 34 lõige 1.

rikkumiste tagajärjed on oma laadilt tagasipööratamatud. Enne kui vastutav töötleja saab teatavas vormis ründest põhjustatud rikkumisest tulenevaid riske *täielikult* hinnata, tuleks tuvastada probleemi algpõhjus, et teha kindlaks, kas jätkuvalt esineb mõni intsidendi põhjustanud nõrkus, mida saab endiselt ära kasutada. Paljudel juhtudel suudab vastutav töötleja kindlaks teha, et intsidendi tagajärjel võib tekkida risk, ja seepärast tuleb sellest teatada. Muudel juhtudel ei ole vaja teavitamisega oodata seni, kuni rikkumisega kaasnevat riski ja rikkumise mõju on täielikult hinnatud, sest täieliku riskihindamise saab läbi viia paralleelselt teavitamisega ja sel viisil saadud teabe saab järelevalveasutusele esitada järk-järgult ilma põhjendamatu viivituseta[9].

9. Rikkumisest tuleks teatada juhul, kui vastutava töötleja arvamuse kohaselt kaasneb sellega risk andmesubjekti õigustele ja vabadustele. Vastutavad töötlejad peavad seda hindama ajal, mil nad rikkumisest teadlikuks saavad. Vastutav töötleja ei peaks ära ootama üksikasjalikku kohtuekspertiisi ega (varajasi) leevendusmeetmeid enne selle hindamist, kas andmetega seotud rikkumine tekitab tõenäoliselt riski ja kas sellest tuleks seega teatada.

10. Kui vastutava töötleja enda hinnangul on risk ebatõenäoline, kuid ilmneb, et risk materialiseerub, siis saab järelevalveasutus kasutada oma parandusvolitusi ja võib määrata karistusi.

11. Kõik vastutavad töötlejad ja volitatud töötlejad peavad olema kehtestanud kavad ja menetlused olukorraks, kui lõppkokkuvõttes on vaja andmetega seotud rikkumisi lahendada. Organisatsioonides peavad olemas olema selged aruandlusahelad ja taastamisprotsessi teatavate aspektide eest vastutavad isikud.

12. Samuti on vastutava töötleja ja volitatud töötleja jaoks äärmiselt oluline oma töötajate koolitamine ja teadlikkus andmekaitseküsimustes, keskendudes isikuandmetega seotud rikkumise haldamisele (isikuandmetega seotud rikkumisjuhtumite tuvastamine, täiendavad meetmed, mida tuleb võtta, jne). Sõltuvalt töötlemistoimingu liigist ja vastutava töötleja suurusest tuleks kõnealust koolitust regulaarselt korrata, käsitledes viimaseid suundumusi ja küberrünnete või muude turvaintsidentide kohta tehtud hoiatusi.

13. Vastutuse ja lõimitud andmekaitse põhimõtted võivad hõlmata analüüsi, millele tuginetakse vastutava töötleja ja volitatud töötleja enda käsiraamatus isikuandmetega seotud rikkumiste käsitlemise kohta, mille eesmärk on teha kindlaks töötlemistoimingu kõikide oluliste etappide iga tahuga seotud faktid. Selline eelnevalt koostatud käsiraamat pakuks palju kiiremini kasutatavat teabeallikat, mis võimaldaks vastutavatel töötlejatel ja volitatud töötlejatel maandada riske ja täita oma kohustusi põhjendamatu viivituseta. See tagaks, et isikuandmetega seotud rikkumise toimumise korral teavad organisatsioonis töötavad inimesed mida teha, ning et intsidentidega tegeletakse tõenäoliselt kiiremini kui olukorras, kus maandamismeetmeid või -kava ei ole kehtestatud.

14. Kuigi allpool esitatud juhtumid on välja mõeldud, on nende aluseks tüüpilised juhtumid, mis põhinevad järelevalveasutuste kollektiivsetel kogemustel seoses andmetega seotud rikkumisest teatamisega. Esitatud analüüsid on konkreetselt seotud vaadeldavate juhtumitega, kuid nende eesmärk on abistada vastutavaid töötlejaid nende enda andmetega seotud rikkumiste hindamisel. Mis tahes erinevustega allpool kirjeldatud juhtumite asjaoludes võivad kaasneda erinevad või kõrgemad riskitasemed, mis seega nõuavad erinevaid või täiendavaid meetmeid. Käesolevates suunistes on juhtumid esitatud rikkumise teatavate kategooriate (nt lunavararünded) järgi. Rikkumise teatava kategooria käsitlemisel on iga juhtumi puhul vaja võtta konkreetseid leevendamismeetmeid. Neid meetmeid ei ole kõikide samasse kategooriasse kuuluvate

[9] Isikuandmete kaitse üldmääruse artikli 33 lõige 4.

rikkumiste all esitatud juhtumianalüüsides tingimata korratud. Samasse kategooriasse kuuluvate juhtumite puhul on esitatud üksnes erinevused. Seepärast tuleks läbi lugeda kõik rikkumise asjaomase kategooria seisukohast asjakohased juhtumid, et teha kindlaks kõik õiged meetmed, mida tuleb võtta, ja neid eristada.

15. Kohustus rikkumine asutusesiseselt dokumenteerida ei sõltu rikkumisega kaasnevatest riskidest ja seda tuleb teha iga juhtumi puhul. Allpool esitatud juhtumite abil püütakse tuua teatavat selgust sellesse, kas rikkumisest tuleks järelevalveasutust ja mõjutatud andmesubjekte teavitada või mitte.

2 LUNAVARA

16. Sage põhjus andmetega seotud rikkumisest teavitamiseks on vastutava töötleja vastu suunatud lunavararünne. Selliste juhtumite puhul krüpteerib ründekood isikuandmed ja seejärel nõuab ründaja vastutavalt töötlejalt dekrüpteerimiskoodi eest lunaraha. Seda liiki ründe võib tavaliselt liigitada kättesaadavusega seotud rikkumiseks, kuid sageli võib esineda ka konfidentsiaalsusega seotud rikkumine.

2.1 JUHTUM nr 1. Lunavara nõuetekohaselt varundatud andmete korral ja ilma andmelekketa

Väikese tootmisettevõtte arvutisüsteemide vastu viidi läbi lunavararünne; nendes süsteemides säilitatavad andmed olid krüpteeritud. Vastutav töötleja kasutas jõudeolekus andmete krüpteerimist, seega säilitati kõiki andmeid, millele lunavara juurde pääses, krüpteeritud kujul, kasutades tehnika tasemel põhinevat krüpteerimisalgoritmi. Ründega ei murtud dekrüpteerimisvõtit, see tähendab ründaja ei suutnud sellele juurde pääseda ega seda kaudselt kasutada. Selle tulemusel oli ründajal juurdepääs vaid krüpteeritud isikuandmetele. Eelkõige ei olnud mõjutatud ettevõtte e-posti süsteem ega ükski sellele juurdepääsemiseks kasutatav klientsüsteem. Ettevõte kasutab intsidendi uurimiseks välise küberturvalisusettevõtja erialateadmisi. Kättesaadavad on logid, milles jälgitakse ettevõttest väljuvaid andmevooge (sealhulgas väljasaadetavaid e-kirju). Pärast logide ja ettevõtte kasutatavate tuvastussüsteemide kogutud andmete analüüsimist tuvastati välise küberturvalisusettevõtja toetusel läbiviidud siseuurimise põhjal *kindlalt*, et ründe toimepanija üksnes krüpteeris andmeid, kuid ei varastanud neid. Logid ei näita ründe ajal väljapoole suunduvat andmevoogu. Rikkumisest mõjutatud isikuandmed käsitlevad ettevõtte kliente ja töötajaid, kokku mõndakümmet isikut. Varundatud andmed olid hõlpsalt kättesaadavad ja andmed taastati mõne tunni jooksul pärast ründe toimumist. Rikkumine ei mõjutanud vastutava töötleja igapäevast tegevust mingil viisil. Töötajatele tehtavates maksetes ega klientide päringute käsitlemisel ei esinenud viivitusi.

17. Selle juhtumi puhul toimus isikuandmetega seotud rikkumise mõiste kohaselt turvanõuete rikkumine, mis põhjustas salvestatud isikuandmete ebaseadusliku muutmise ja neile loata juurdepääsu.

2.1.1 JUHTUM nr 1. Eelnevad meetmed ja riskihindamine

18. Nagu kõikide välisteguritest tingitud riskide puhul saab lunavararünde edukuse tõenäosust oluliselt vähendada, karmistades turvanõudeid keskkonnas, kus andmeid kontrollitakse. Enamiku sellistest rikkumistest saab ära hoida, tagades, et võetud on asjakohased korralduslikud, füüsilised ja tehnoloogilised turvameetmed. Sellised meetmed on näiteks nõuetekohane paigahaldus ja asjakohase pahavaravastase tuvastussüsteemi kasutamine. Nõuetekohaste ja eraldi varukoopiate olemasolu aitab leevendada tagajärgi juhul, kui toimuma peaks edukas rünne. Peale selle aitab seda liiki ründeid ära hoida ja tuvastada töötajate turvaalase väljaõppe, koolituse ja teadlikkuse suurendamise programm. (Soovitatavate meetmete loetelu on esitatud punktis 2.5.) Teiste seas on üks kõige olulisemaid meetmeid nõuetekohane paigahaldus, millega

tagatakse, et süsteemid on ajakohastatud ja kõik kasutatavate süsteemide teadaolevad nõrkused on parandatud, sest enamiku lunavararünnete puhul kasutatakse ära hästi teada olevaid nõrkusi.

19. Riskide hindamisel peaks vastutav töötleja ründe võimalike tagajärgede mõistmiseks rikkumist uurima ja tegema kindlaks ründekoodi liigi. Muu hulgas tuleb võtta arvesse riski, et toimus andmeleke, millest süsteemide logidesse ei ole jälge jäänud.

20. Selle näite puhul oli ründajal juurdepääs isikuandmetele ning rikuti krüpteeritud kujul isikuandmeid sisaldava šifferteksti konfidentsiaalsust. Ründaja ei suuda aga vähemalt praegu lugeda ega kasutada mingeid andmeid, mis võisid lekkida. Vastutava töötleja kasutatud krüpteerimistehnika vastab tehnika tasemele. Krüpteerimisvõtit ei murtud ja eelduste kohaselt ei saa seda kindlaks teha ka muude vahenditega. Selle tulemusel piirdub konfidentsiaalsusrisk füüsiliste isikute õigustele ja vabadustele minimaalsega, sest tõkestatud on krüptoanalüütiline tegevus, mille tagajärjel saab krüpteeritud andmed edaspidi loetavaks muuta.

21. Vastutav töötleja peaks kaaluma ründest tulenevaid riske üksikisikutele[10]. Esitatud juhtumi puhul tunduvad riskid andmesubjektide õigustele ja vabadustele tulenevat asjaolust, et isikuandmed ei ole kättesaadavad, ning isikuandmete konfidentsiaalsust ei ole rikutud[11]. Selle näite puhul leevendati rikkumise kahjulikku mõju suhteliselt kiiresti pärast rikkumise toimumist. Nõuetekohase varundussüsteemi[12] olemasolu vähendab rikkumise mõju ja antud juhul suutis vastutav töötleja seda tõhusalt kasutada.

22. Mis puudutab tagajärgede tõsidust andmesubjektidele, siis saab tuvastada vaid ebaolulised tagajärjed, sest mõjutatud andmed taastati mõne tunni jooksul ning rikkumine ei mõjutanud vastutava töötleja igapäevast tegevust mingil viisil ega avaldanud olulist mõju andmesubjektidele (näiteks töötajatele maksete tegemisele ega klientide päringute käsitlemisele).

2.1.2 JUHTUM nr 1. Leevendamine ja kohustused

23. Kui andmed ei ole varundatud, siis ei ole vastutaval töötlejal isikuandmete kaotsimineku korvamiseks palju võimalusi ja andmed tuleb uuesti koguda. Kõnealusel konkreetsel juhul sai aga ründe mõju tõhusalt piirata, lähtestades kõik rikutud süsteemid puhtasse olekusse, mille puhul on teada, et need ei sisalda ründekoodi,

---

[10] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt artikli 29 töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679, WP248 rev. 01 (Euroopa Andmekaitsenõukogu poolt heaks kiidetud), https://ec.europa.eu/newsroom/article29/items/611236, lk 9.

[11] Tehniliselt hõlmab andmete krüpteerimine juurdepääsu algsetele andmetele ja lunavara puhul algsete andmete kustutamist – andmete krüpteerimiseks ja algsete andmete eemaldamiseks peab lunavara neile juurde pääsema. Ründaja võib enne algsete andmete kustutamist need kopeerida, kuid alati isikuandmetest väljavõtet ei tehta. Vastutava töötleja uurimise edenedes võib ilmneda uut teavet, mille tagajärjel see hinnang muutub. Juurdepääsul, mille tulemuseks on isikuandmete ebaseaduslik hävitamine, kaotsiminek, muutmine või loata avalikustamine või turvarisk andmesubjektile isegi ilma andmete tõlgendamiseta, võivad olla sama tõsised tagajärjed kui juurdepääsul, millega kaasneb isikuandmete tõlgendamine.

[12] Varundamismenetlused peaksid olema struktureeritud, järjepidevad ja korratavad. Varundamismenetluste näited on 3-2-1 meetod ja nn vanaisa-isa-poeg meetod. Kõikide meetodite puhul tuleks alati katsetada, kui tõhusad need on oma hõlmavuse poolest ja juhul, kui andmeid on vaja taastada. Samuti tuleks süsteemi terviklikkuse tagamiseks katsetamist teatavate ajavahemike tagant korrata, eelkõige siis, kui töötlemistoimingus või selle asjaoludes tehakse muudatusi.

kõrvaldades nõrkused ja taastades mõjutatud andmed kiiresti pärast rünnet. Ilma varundamiseta lähevad andmed kaotsi ja rikkumise raskusaste võib kasvada, sest suureneda võivad riskid või mõju üksikisikutele.

24. Rikkumise analüüsimisel on oluline tegur aeg, mis kulub andmete tõhusaks taastamiseks hõlpsalt kättesaadavast varukoopiast. Rikutud andmete taastamise sobiliku ajakava täpsustamine sõltub asjaomase rikkumise konkreetsetest asjaoludest. Isikuandmete kaitse üldmääruses on märgitud, et isikuandmetega seotud rikkumisest tuleb teavitada põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul. Selle põhjal võib järeldada, et ühelgi juhul ei ole soovitatav 72tunnist ajalist piirangut ületada, kuid kõrge riskitasemega juhtumite käsitlemisel võib ka selle tähtaja järgimist pidada ebarahuldavaks.

25. Käesoleval juhul tegi vastutav töötleja põhjaliku riskihindamise ja intsidentidele reageerimise protsessi põhjal kindlaks, et rikkumisega tõenäoliselt ei kaasne riski füüsiliste isikute õigustele ja vabadustele, seega ei ole vaja andmesubjekte ega järelevalveasutust rikkumisest teavitada. Nagu kõikide andmetega seotud rikkumiste puhul, tuleb see aga kooskõlas artikli 33 lõikega 5 dokumenteerida. Samuti võib organisatsioonil olla vaja ajakohastada oma korralduslikke ja tehnilisi isikuandmete turbe meetmeid ning riskimaandamismeetmeid ja -menetlusi (või võib järelevalveasutus seda hiljem nõuda). Selle ajakohastamise ja maandamise raames peaks organisatsioon rikkumist põhjalikult uurima ning tegema kindlaks ründe toimepanija põhjused ja tema kasutatud meetodid, et vältida sarnaseid sündmusi tulevikus.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

2.2 JUHTUM nr 2. Lunavara nõuetekohaselt varundamata andmete korral

Ühe arvuti vastu, mida kasutab põllumajandusettevõte, viidi läbi lunavararünne ja ründaja krüpteeris selles sisalduvad andmed. Ettevõte kasutab oma võrgu jälgimiseks välise küberturvalisusettevõtja erialateadmisi. Kättesaadavad on logid, milles jälgitakse ettevõttest väljuvaid andmevooge (sealhulgas väljasaadetavaid e-kirju). Pärast logide ja muude tuvastussüsteemide kogutud andmete analüüsimist tuvastati küberturvalisusettevõtja abil läbiviidud siseuurimise põhjal, et ründe toimepanija üksnes krüpteeris andmeid, kuid ei varastanud neid. Logid ei näita ründe ajal väljapoole suunduvat andmevoogu. Rikkumisest mõjutatud isikuandmed käsitlevad ettevõtte töötajaid ja kliente, kokku mõndakümmet isikut. Mõjutatud ei olnud mingid andmete eriliigid. Elektroonilises vormis varukoopiaid ei olnud. Enamik andmeid taastati paberkandjal varukoopiate põhjal. Andmete taastamiseks kulus viis tööpäeva ja sellega kaasnesid väikesed viivitused klientide tellimuste täitmisel.

2.2.1 JUHTUM nr 2. Eelnevad meetmed ja riskihindamine

26. Vastutav töötleja oleks pidanud võtma samasugused eelnevad meetmed, nagu on kirjeldatud punktides 2.1 ja 2.9. Peamine erinevus võrreldes eelneva juhtumiga on elektrooniliste varukoopiate puudumine ja asjaolu, et jõudeolekus andmed ei olnud krüpteeritud. Selle tulemusel esineb järgnevates sammudes olulisi erinevusi.

27. Riskide hindamisel peaks vastutav töötleja ründe võimalike tagajärgede mõistmiseks sissetungimise meetodit uurima ja tegema kindlaks ründekoodi liigi. Käesoleva näite puhul krüpteeriti lunavaraga isikuandmed, ilma et need oleksid lekkinud. Selle tagajärjel tunduvad riskid andmesubjektide õigustele ja vabadustele tulenevat asjaolust, et isikuandmed ei ole kättesaadavad, ning isikuandmete konfidentsiaalsust ei ole rikutud. Riski kindlakstegemiseks on äärmiselt oluline põhjalikult uurida tulemüüri logisid ja selle mõju. Taotluse korral peaks vastutav töötleja esitama nende uurimiste faktilised järeldused.

28. Vastutav töötleja peab arvesse võtma, et kui rünne on keerulisem, suudab pahavara logifaile redigeerida ja selle jäljed kõrvaldada. Kuna logisid ei edastata ega kopeerita kesksesse logiserverisse, ei saa vastutav töötleja seega isegi pärast põhjalikku uurimist, mille käigus tehti kindlaks, et ründaja ei varastanud isikuandmeid, väita, et logisissekande puudumine tõendab andmelekke puudumist, ja seepärast ei saa täielikult eirata konfidentsiaalsusega seotud rikkumise tõenäosust.

29. Vastutav töötleja peaks hindama selle rikkumisega kaasnevaid riske[13] juhul, kui ründaja andmetele juurde pääses. Riskihindamise käigus peaks vastutav töötleja arvesse võtma ka rikkumisest mõjutatud isikuandmete laadi, tundlikkust, mahtu ja konteksti. Käesoleval juhul ei mõjutatud mingeid isikuandmete eriliike ning rikkumisega seotud andmete hulk ja mõjutatud andmesubjektide arv on väike.

30. Loata juurdepääsu kohta täpse teabe kogumine on äärmiselt tähtis riskitaseme kindlakstegemiseks ja uue ründe või ründe jätkumise vältimiseks. Kui andmeid oleks andmebaasist kopeeritud, oleks see ilmselgelt olnud riske suurendav tegur. Kui ebaseadusliku juurdepääsu konkreetsete asjaolude suhtes valitseb ebakindlus, tuleks arvestada halvima stsenaariumiga ja hinnata riske vastavalt sellele.

31. Asjaolu, et andmebaasi ei varundatud, saab käsitada riske suurendava tegurina, sõltuvalt andmetele juurdepääsu puudumise tagajärjel andmesubjektidele avalduvate tagajärgede raskusastmest.

2.2.2 JUHTUM nr 2. Leevendamine ja kohustused

32. Kui andmed ei ole varundatud, siis ei ole vastutaval töötlejal isikuandmete kaotsimineku korvamiseks palju võimalusi ja andmed tuleb uuesti koguda, kui ei saa kasutada mõnda muud allikat (nt tellimuste kinnituseks saadetud e-kirju). Ilma varundamata võivad andmed kaotsi minna ja rikkumise raskusaste sõltub üksikisikutele avalduvast mõjust.

33. Andmete taastamine ei tohiks olla ülemäära keeruline,[14] kui andmed on paberkandjal jätkuvalt kättesaadavad, kuid elektroonilise varuandmebaasi puudumist arvesse võttes peetakse järelevalveasutuse teavitamist vajalikuks, sest andmete taastamiseks kulus teatav aeg ja see võib põhjustada mõningaid viivitusi klientide tellimuste täitmisel ning suur osa metaandmeid (nt logid, ajatemplid) ei pruugi olla taastatavad.

34. Andmesubjektide rikkumisest teavitamine võib sõltuda ka ajast, mille jooksul isikuandmed ei ole kättesaadavad, ja probleemidest, mis võivad selle tulemusel vastutava töötleja tegevuses esineda (nt viivitused töötajatele maksete ülekandmisel). Kuna sellised viivitused maksete tegemisel ja tarnetes võivad põhjustada isikutele, kelle andmeid rikuti, rahalist kahju, siis võib väita ka seda, et rikkumisega kaasneb tõenäoliselt suur risk. Samuti ei pruugi olla võimalik vältida andmesubjektide teavitamist, kui krüpteeritud andmete taastamiseks on vaja nende panust.

35. Käesolev juhtum on näide lunavararündest, mis tekitab riski andmesubjektide õigustele ja vabadustele, kuid see risk ei ole suur. Juhtum tuleb kooskõlas artikli 33 lõikega 5 dokumenteerida ja sellest tuleb kooskõlas artikli 33 lõikega 1 järelevalveasutusele teatada. Samuti võib organisatsioonil olla vaja ajakohastada oma

[13] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

[14] See sõltub isikuandmete keerukusest ja struktuurist. Kõige keerulisemate stsenaariumide puhul võib andmetervikluse taastamine, metaandmetega järjepidevuse ja andmestruktuurides õigete seoste tagamine ning andmete õigsuse kontrollimine nõuda märkimisväärseid ressursse ja pingutusi.

korralduslikke ja tehnilisi isikuandmete turbe meetmeid ning riskimaandamismeetmeid ja -menetlusi (või võib järelevalveasutus seda nõuda).

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	X

2.3 JUHTUM nr 3. Lunavara varundatud andmete korral ja ilma andmelekketa haigla puhul

Haigla/tervisekeskuse infosüsteemi vastu viidi läbi lunavararünne ja ründaja krüpteeris olulise osa selles sisalduvatest andmetest. Ettevõte kasutab oma võrgu jälgimiseks välise küberturvalisusettevõtja erialateadmisi. Kättesaadavad on logid, milles jälgitakse ettevõttest väljuvaid andmevooge (sealhulgas väljasaadetavaid e-kirju). Pärast logide ja muude tuvastussüsteemide kogutud andmete analüüsimist tuvastati küberturvalisusettevõtja abil läbiviidud siseuurimise põhjal, et ründe toimepanija üksnes krüpteeris andmeid, kuid ei varastanud neid. Logid ei näita ründe ajal väljapoole suunduvat andmevoogu. Rikkumisest mõjutatud isikuandmed käsitlevad töötajaid ja patsiente, see tähendab tuhandeid isikuid. Olemas on elektroonilises vormis varukoopiad. Enamik andmeid taastati, kuid see toiming kestis kaks tööpäeva ning selle tagajärjel esines suuri viivitusi patsientide ravis, kuna operatsioonid tühistati / lükati edasi, ja süsteemide kättesaadamatuse tõttu langes teenuse tase.

2.3.1 JUHTUM nr 3. Eelnevad meetmed ja riskihindamine

36. Vastutav töötleja oleks pidanud võtma samasugused eelnevad meetmed, nagu on kirjeldatud punktides 2.1 ja 2.5. Peamine erinevus eelmise juhtumiga seisneb väga tõsistes tagajärgedes olulisele osale andmesubjektidest[15].

37. Rikutud andmete hulk ja mõjutatud andmesubjektide arv on suur, sest haiglad töötlevad üldjuhul suures koguses andmeid. Andmete kättesaadamatus avaldab suurt mõju olulisele osale andmesubjektidest. Peale selle esineb väga tõsine jääkrisk patsiendiandmete konfidentsiaalsusele.

38. Rikkumise liik ning mõjutatud isikuandmete laad, tundlikkus ja maht on olulised. Kuigi andmed olid varundatud ja need oli võimalik paari päevaga taastada, esineb jätkuvalt suur risk andmesubjektidele avalduvate tagajärgede tõsiduse tõttu, mis tuleneb andmete kättesaadamatusest ründe ajal ja järgnevatel päevadel.

2.3.2 JUHTUM nr 3. Leevendamine ja kohustused

39. Järelevalveasutuse teavitamist peetakse vajalikuks, sest tegemist on isikuandmete eriliikidega ja andmete taastamiseks võib kuluda palju aega, mille tagajärjel tekib patsientide ravis olulisi viivitusi. Rikkumise mõju tõttu patsientidele tuleb andmesubjekte isegi pärast krüpteeritud andmete taastamist rikkumisest teavitada. Kuigi krüpteeriti kõikide viimastel aastatel haiglas ravitud patsientide andmed, mõjutas see ainult neid patsiente, keda oli kavas ravida haiglas sel ajal, mil arvutisüsteem ei olnud kättesaadav. Vastutav töötleja peab neid patsiente andmetega seotud rikkumisest otse teavitama. Teiste patsientide teavitamine, kellest osad võisid haiglas viibida enam kui 20 aastat tagasi, ei pruugi olla vajalik tulenevalt artikli 34 lõike 3 punktis c sätestatud erandist. Sellisel juhul tuleks selle asemel esitada avalik teade[16] või võtta muu sarnane meede,

[15] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

[16] Isikuandmete kaitse üldmääruse põhjenduses 86 on selgitatud järgmine: „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.“

millega andmesubjekte sama tõhusalt teavitatakse. Käesoleva juhtumi puhul peaks haigla lunavararünde ja selle mõju avalikustama.

40. See juhtum on näide lunavararündest, mis tekitab suure riski andmesubjektide õigustele ja vabadustele. Juhtum tuleb kooskõlas artikli 33 lõikega 5 dokumenteerida ning sellest tuleb teatada järelevalveasutustele kooskõlas artikli 33 lõikega 1 ja andmesubjektidele kooskõlas artikli 34 lõikega 1. Samuti on organisatsioonil vaja ajakohastada oma korralduslikke ja tehnilisi isikuandmete turbe meetmeid ning riskimaandamismeetmeid ja -menetlusi.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

2.4 JUHTUM nr 4. Lunavara varundamata andmete korral ja koos andmelekkega

Ühistranspordiettevõtte serveri vastu viidi läbi lunavararünne ja ründaja krüpteeris selles sisalduvad andmed. Siseuurimise järelduste kohaselt ründe toimepanija lisaks andmete krüpteerimisele ka varastas need. Mis puudutab rikutud andmete liiki, siis oli tegemist klientide ja töötajate ning tuhandete ettevõtte teenuseid kasutavate (nt elektrooniliselt pileteid ostvate) inimeste isikuandmetega. Lisaks põhilistele isikuandmetele puudutas rikkumine ka isikutunnistuste numbreid ja finantsandmeid, näiteks krediitkaartide andmed. Olemas oli varuandmebaas, kuid ründaja krüpteeris ka selle.

2.4.1 JUHTUM nr 4. Eelnevad meetmed ja riskihindamine

41. Vastutav töötleja oleks pidanud võtma samasugused eelnevad meetmed, nagu on kirjeldatud punktides 2.1 ja 2.5. Kuigi olemas olid varundatud andmed, mõjutas rünne ka neid. Juba see korraldus iseenesest tõstatab küsimusi vastutava töötleja varasemate IT-turbe meetmete kvaliteedi kohta, mis tuleks uurimise käigus läbi vaadata, sest hästi kavandatud varundussüsteemis peab olema turvaliselt salvestatud mitu varukoopiat, millele põhisüsteemist puudub juurdepääs, vastasel korral võib sama rünne ka neid mõjutada. Peale selle võib lunavararünnete avastamiseks kuluda mitu päeva, mille jooksul lunavara harva kasutatavaid andmeid aeglaselt krüpteerib. Selle tulemusel võivad mitmed varukoopiad olla kasutud, seega tuleks ka varukoopiaid teha korrapäraselt ja need peaksid olema isoleeritud. See suurendaks taastamise tõenäosust, kuigi kaotatud andmete hulk kasvaks.

42. Kõnealune rikkumine ei ole seotud mitte üksnes andmete kättesaadavuse, vaid ka konfidentsiaalsusega, sest ründaja võis andmeid muuta ja/või neid serverist kopeerida. Seepärast kaasneb seda liiki rikkumisega suur risk[17].

43. Isikuandmete laad, tundlikkus ja maht suurendavad riske veelgi, sest nii mõjutatud isikute arv kui ka mõjutatud isikuandmete koguhulk on suur. Lisaks põhilistele isikuandmetele puudutas rikkumine ka isikut tõendavaid dokumente ja finantsandmeid, näiteks krediitkaartide andmed. Seda liiki andmetega seotud rikkumine kujutab iseenesest suurt riski ja kui neid andmeid töödeldakse koos, siis võib neid muu hulgas kasutada identiteedivarguseks või pettuseks.

[17] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

44. Serveri loogikas või organisatsioonilistes kontrollimeetmetes esinevate vigade tõttu mõjutas lunavara varufaile, mis välistas andmete taastamise ja suurendas riski.

45. Selline andmetega seotud rikkumine kujutab suurt riski üksikisikute õigustele ja vabadustele, sest sellega võib kaasneda nii materiaalne kahju (nt rahaline kahju mõjutatud krediitkaardiandmete tõttu) kui ka mittemateriaalne kahju (nt identiteedivargus või pettus mõjutatud isikutunnistuse andmete tõttu).

2.4.2 JUHTUM nr 4. Leevendamine ja kohustused

46. Äärmiselt oluline on teavitada andmesubjekte, et nad saaksid astuda vajalikke samme materiaalse kahju ennetamiseks (nt sulgeda oma krediitkaardid).

47. Lisaks rikkumise dokumenteerimisele kooskõlas artikli 33 lõikega 5 on käesoleva juhtumi puhul kohustuslik ka järelevalveasutuse teavitamine (artikli 33 lõige 1) ning samuti peab vastutav töötleja teatama rikkumisest andmesubjektidele (artikli 34 lõige 1). Viimast võib teha näost näkku, kuid isikute puhul, kelle isikuandmed ei ole kättesaadavad, peaks vastutav töötleja tegema seda avalikult, näiteks avaldades teate oma veebisaidil, tingimusel et sellise teavitamisega ei kaasneks andmesubjektidele täiendavaid negatiivseid tagajärgi. Viimasel juhul tuleb esitada täpne ja selge teade, mis on vastutava töötleja kodulehel selgelt nähtav ja milles viidatakse täpselt isikuandmete kaitse üldmääruse asjakohastele sätetele. Samuti võib organisatsioonil olla vaja ajakohastada oma korralduslikke ja tehnilisi isikuandmete turbe meetmeid ning riskimaandamismeetmeid ja -menetlusi.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

2.5 Korralduslikud ja tehnilised meetmed lunavararünnete mõju ennetamiseks/leevendamiseks

48. Asjaolu, et toimuda võis lunavararünne, on üldjuhul märk ühest või mitmest nõrkusest vastutava töötleja süsteemis. See kehtib ka selliste lunavaraga seotud juhtumite suhtes, mille puhul isikuandmed on krüpteeritud, kuid need ei ole lekkinud. Olenemata ründe tulemustest ja tagajärgedest ei saa piisavalt rõhutada andmeturbesüsteemi kõikehõlmava ja eelkõige IT-turbele keskenduva hindamise tähtsust. Kindlakstehtud nõrkused ja turvaaugud tuleb dokumenteerida ja viivitamata kõrvaldada.

49. Soovitatavad meetmed.

(Alljärgnevate meetmete loetelu ei ole lõplik ega kõikehõlmav. Pigem on selle eesmärk anda ideid ennetamiseks ja võimalikeks lahendusteks. Iga töötlemistoiming on erinev, seega peab vastutav töötleja otsustama, millised meetmed on asjaomase olukorra puhul kõige sobilikumad.)

- Serverites, klientmasinates, aktiivsetes võrgukomponentides ja kõikides muudes sama kohtvõrguga ühendatud masinates (sealhulgas WiFi-seadmetes) oleva püsivara, operatsioonisüsteemi ja rakendustarkvara ajakohane hoidmine. Selle tagamine, et kehtestatud on asjakohased IT-turbemeetmed ja et need on tõhusad, ning nende korrapärane ajakohastamine töötlemise või asjaolude muutudes või arenedes. See hõlmab üksikasjalike logide pidamist rakendatud paikade ja nende ajatemplite kohta.
- Töötlemissüsteemide ja -taristu kavandamine ja korraldamine nii, et andmesüsteeme ja võrke saaks segmentida või isoleerida, eesmärgiga vältida pahavara levimist organisatsiooni sees ja välistesse süsteemidesse.
- Ajakohase, turvalise ja läbiproovitud varundusmenetluse olemasolu. Keskmise tähtajaga ja pikaajaliselt säilitatavate varukoopiate kandjaid tuleks säilitada eraldi operatiivandmetest ja nii, et need oleksid isegi

eduka ründe korral kolmandatele isikutele kättesaamatud (näiteks igapäevane sammvarundus ja iganädalane täielik varundus).

- Sobiliku, ajakohase, tõhusa ja integreeritud pahavaravastase tarkvara omamine/hankimine.
- Sobiliku, ajakohase, tõhusa ja integreeritud tulemüüri ning sissetungi tuvastamise ja tõrjumise süsteemi omamine. Võrguliikluse suunamine läbi tulemüüri / sissetungi tuvastamise süsteemi isegi kodukontori või mobiilivõrgu puhul (nt internetti juurdepääsemisel organisatsiooni turvamehhanismidega seotud VPN-ühenduste kasutamine).
- Töötajate koolitamine IT-rünnete äratundmise ja ennetamise meetodite alal. Vastutav töötleja peaks pakkuma vahendeid selle kindlakstegemiseks, kas muude sidevahendite kaudu saadud e-kirjad ja sõnumid on autentsed ja usaldusväärsed. Töötajaid tuleks koolitada, et nad tunneksid ära sellise ründe toimumise, oskaksid otspunkti võrgust eemaldada ja oleksid teadlikud oma kohustusest sellest viivitamata turvaametnikule teatada.
- Ründekoodi liigi kindlakstegemise vajaduse rõhutamine, et mõista ründe tagajärgi ja suuta võtta õigeid meetmeid riski maandamiseks. Juhul, kui lunavararünne on olnud edukas ja puuduvad varukoopiad, võib andmete taastamiseks kasutada näiteks selliseid vahendeid, mida pakub projekt „No more ransom“ (nomoreransom.org). Kui aga on olemas varukoopiad, siis on soovitatav taastada andmed nende põhjal.
- Kõikide logide edastamine või kopeerimine kesksesse logiserverisse (mis võib hõlmata logikannete allkirjastamist või krüptograafilise ajatempliga varustamist).
- Tugev krüpteerimine ja mitmikautentimine, eelkõige haldusjuurdepääsu korral IT-süsteemidele, ning võtmete ja paroolide asjakohane haldamine.
- Korrapärane nõrkuste ja läbistustestimine.
- Organisatsioonis küberturbe intsidentide lahendamise üksuse (CSIRT) või infoturbeintsidentidega tegeleva rühma (CERT) loomine või kollektiivse CSIRTi/CERTiga liitumine. Intsidentidele reageerimise kava, avariitaastekava ja talitluspidevuse kava koostamine ning nende põhjaliku testimise tagamine.
- Vastumeetmete hindamisel tuleb riskihinnang läbi vaadata ning seda testida ja ajakohastada.

3 ANDMELEKET HÕLMAVAD RÜNDED

50. Ründed, mille puhul kasutatakse ära vastutava töötleja poolt kolmandatele isikutele interneti kaudu pakutavates teenustes esinevaid nõrkusi, näiteks ründed, mida viiakse läbi süstrünnete (nt SQL süstid, teehüpped), veebisaidi rikkumise ja samasuguste meetoditega, võivad sarnaneda lunavararünnetega selle poolest, et risk tuleneb loata kolmanda isiku tegevusest, kuid selliste rünnete eesmärk on tavaliselt isikuandmete kopeerimine, lekitamine ja kuritarvitamine teataval pahatahtlikul eesmärgil. Seega on nende puhul peamiselt tegemist konfidentsiaalsusega, ja võimalik, et ka andmete terviklusega seotud rikkumistega. Aga kui vastutav töötleja on teadlik seda laadi rikkumiste tunnustest, saab ta kasutada mitmeid meetmeid, mis võivad oluliselt vähendada ründe eduka läbiviimise tõenäosust.

3.1 JUHTUM nr 5. Töökohale kandideerimise taotluste andmete leke veebisaidilt

Tööhõivebüroo vastu korraldati küberrünne, mille käigus paigaldati tema veebisaidile ründekood. Selle ründekoodiga tehti elektrooniliste töökohale kandideerimise taotluste vormides esitatud ja veebiserveris talletatud isikuandmed kättesaadavaks loata isiku(te)le. See võis mõjutada 213 sellist vormi, ent pärast mõjutatud andmete analüüsimist tehti kindlaks, et rikkumine ei mõjutanud mingeid andmete eriliike. Konkreetne paigaldatud pahavara tööriistakomplekt sisaldas funktsioone, mis võimaldasid ründajal eemaldada andmelekke ajaloo ning samuti jälgida serveris toimuvat töötlemist ja hõivata isikuandmeid. Tööriistakomplekt avastati alles kuu aega pärast selle paigaldamist.

3.1.1 JUHTUM nr 5. Eelnevad meetmed ja riskihindamine

51. Vastutava töötleja keskkonna turvalisus on äärmiselt oluline, sest enamiku sellistest rikkumistest saab ära hoida, tagades et kõiki süsteeme pidevalt ajakohastatakse, et tundlikud andmed on krüpteeritud ja et rakenduste väljatöötamisel lähtutakse kõrgetest turvastandarditest, nagu tugev autentimine, jõurünnetevastased meetmed ja kasutajate sisendandmetest väljamurd või nende puhastamine[18] jms. Seda liiki nõrkuste ennetavaks avastamiseks ja kõrvaldamiseks on vaja ka regulaarseid IT-turbe auditeid, nõrkuste hindamisi ja läbistustestimisi. Selle konkreetse juhtumi puhul oleksid koodisüsti aidanud avastada failide tervikluse jälgimise vahendid tarbekeskkonnas. (Soovitatavate meetmete loetelu on esitatud punktis 3.7.)

52. Vastutav töötleja peaks rikkumise uurimist alati alustama ründe liigi ja meetodite kindlakstegemisest, et hinnata, milliseid meetmeid tuleb võtta. Selleks, et see oleks kiire ja tõhus, peaks vastutav töötleja olema koostanud intsidentidele reageerimise kava, milles on täpsustatud sujuvad ja vajalikud sammud intsidendi kontrolli alla saamiseks. Käesoleva konkreetse juhtumi puhul oli ründe näol tegemist riski suurendava teguriga, sest lisaks andmete konfidentsiaalsuse rikkumisele olid sissetungijal vahendid süsteemis muudatuste tegemiseks, mille tulemusel sattus kahtluse alla ka andmeterviklus.

53. Hinnata tuleks rikkumisest mõjutatud isikuandmete laadi, tundlikkust ja mahtu, et teha kindlaks, mil määral rikkumine andmesubjekte mõjutas. Kuigi mõjutatud ei olnud isikuandmete eriliigid, sisaldavad andmed, millele juurde pääseti, üksikisikute kohta elektroonilistest vormidest pärit olulist teavet ning selliseid andmeid saab mitmel viisil väärkasutada (soovimatu turustamine, identiteedivargus jne), seega peaks tagajärgede tõsidus suurendama riski andmesubjektide õigustele ja vabadustele[19].

3.1.2 JUHTUM nr 5. Leevendamine ja kohustused

54. Võimaluse korral tuleks pärast probleemi lahendamist võrrelda andmebaasi turvalises varukoopias salvestatud andmebaasiga. Rikkumise põhjal saadud kogemusi tuleks arvesse võtta IT-taristu ajakohastamisel. Vastutav töötleja peaks viima kõik mõjutatud IT-süsteemid tagasi teadaolevalt puhtasse olekusse, kõrvaldama nõrkuse ja võtma tulevikus sarnaste andmetega seotud rikkumiste vältimiseks uusi turvameetmeid, näiteks kontrollima failide terviklust ja viima läbi turvaauditeid. Kui isikuandmed mitte üksnes ei lekkinud, vaid need ka kustutati, siis peab vastutav töötleja võtma süstemaatilisi meetmeid isikuandmete taastamiseks nende rikkumisele eelnenud olekus. Vaja võib olla rakendada täielikku varundamist, teha täiendavaid muudatusi ja seejärel töötlemine pärast viimast sammvarundust uuesti läbi

[18] Kasutajate sisendandmetest väljamurd või nende puhastamine on sisendvalideerimise vorm, millega tagatakse, et infosüsteemi sisestatakse ainult nõuetekohases vormingus andmeid.

[19] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

viia, milleks vastutav töötleja peab olema suuteline alates viimasest varundamisest tehtud muudatusi dubleerima. Selleks võib olla vajalik, et vastutava töötleja süsteem on kavandatud säilitama igapäevaseid sisendfaile juhuks, kui neid on vaja uuesti töödelda, ning et kehtestatud on usaldusväärne salvestamismeetod ja sobilik säilitamispõhimõte.

55. Eespool kirjeldatut arvesse võttes ja kuna tõenäoliselt kaasneb rikkumisega suur risk füüsiliste isikute õigustele ja vabadustele, tuleks andmesubjekte rikkumisest kindlasti teavitada (artikli 34 lõige 1), mis ilmselgelt tähendab seda, et kaasata tuleks ka asjaomane järelevalveasutus (asjaomased järelevalveasutused), teatades neile andmetega seotud rikkumisest. Rikkumise dokumenteerimine on isikuandmete kaitse üldmääruse artikli 33 lõike 5 alusel kohustuslik ja see hõlbustab olukorra hindamist.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

3.2 JUHTUM nr 6. Veebisaidilt räsitud parooli leke

SQL süstiga seotud nõrkust kasutati ära juurdepääsu saamiseks kokandusveebisaidi serveri andmebaasile. Kasutajatel võimaldati valida kasutajanimedena vaid meelevaldseid pseudonüüme. Sel eesmärgil ei soovitatud kasutada e-posti aadresse. Andmebaasis salvestatud paroole räsiti tugeva algoritmiga ja soola ei rikutud. Mõjutatud andmed hõlmasid 1 200 kasutaja räsitud paroole. Turvalisuse tagamiseks teavitas vastutav töötleja andmesubjekte rikkumisest e-kirja teel ja palus neil oma paroole muuta, eelkõige juhul, kui sama parooli kasutati muudes teenustes.

3.2.1 JUHTUM nr 6. Eelnevad meetmed ja riskihindamine

56. Selle konkreetse juhtumi puhul rikuti andmete konfidentsiaalsust, kuid andmebaasi kasutamise paroole räsiti ajakohase meetodiga, mis vähendab isikuandmete laadi, tundlikkuse ja mahuga seotud riski. Käesolev juhtum ei tekita riski andmesubjektide õigustele ja vabadustele.

57. Peale selle ei rikutud andmesubjektide kontaktteavet (nt e-posti aadresse või telefoninumbreid), mis tähendab, et puudub märkimisväärne risk, et andmesubjektide suhtes püütakse läbi viia pettusi (nt andmepüügiga seotud e-kirjade või pettuse eesmärgil saadetud tekstisõnumite ja telefonikõnede saamine). Juhtum ei olnud seotud isikuandmete eriliikidega.

58. Teatavaid kasutajanimesid võib käsitada isikuandmetena, kuid veebisaidi sisu tõttu ei ole võimalik luua negatiivseid seoseid. Samal ajal tuleb tähele panna, et riskihindamine võib muutuda,[20] kui veebisaidi ja nende andmete liigi tõttu, millele juurde pääseti, võivad avalikuks saada isikuandmete eriliigid (nt erakonna või ametiühingu veebisaidi puhul). Tehnika tasemel krüpteerimise kasutamine võib leevendada rikkumise kahjulikku mõju. Piiratud arvu sisselogimiskatsete lubamisega välistatakse sisselogimisel jõurünnakatsete edukus, vähendades seega suurel määral selliste ründajate põhjustatud riske, kellele kasutajanimed on juba teada.

3.2.2 JUHTUM nr 6. Leevendamine ja kohustused

59. Mõnel juhul võib andmesubjektide teavitamist käsitada leevendava tegurina, sest ka andmesubjektidel on võimalik võtta vajalikke meetmeid rikkumisega kaasneva edasise kahju vältimiseks, näiteks oma parooli

[20] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

muutmise teel. Käesoleva juhtumi puhul ei olnud teavitamine kohustuslik, kuid paljudel juhtudel saab seda pidada heaks tavaks.

60. Vastutav töötleja peaks nõrkuse kõrvaldama ja rakendama uusi turvameetmeid sarnaste andmetega seotud rikkumiste vältimiseks tulevikus, näiteks viies läbi veebisaidi süstemaatilisi turvaauditeid.

61. Rikkumine tuleb kooskõlas artikli 33 lõikega 5 dokumenteerida, kuid sellest teavitamist ei nõuta.

62. Samuti on tungivalt soovitatav igal juhul teavitada paroole hõlmavast rikkumisest andmesubjekte, isegi kui paroolide säilitamiseks kasutati tehnika tasemele vastava algoritmiga soolatud räsi. Eelistatav on kasutada autentimismeetodeid, millega välistatakse paroolide töötlemise vajadus serveri poolel. Andmesubjektidele tuleks anda võimalus võtta asjakohaseid meetmeid seoses nende enda paroolidega.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

3.3 JUHTUM nr 7. Kontovargusega seotud rünne panga veebisaidil

Panga ühe elektrooniliste pangateenuste veebisaidi vastu korraldati küberrünne. Ründe eesmärk oli loendada sisselogijate kõik võimalikud kasutajatunnused, kasutades kindlaksmääratud lihtparoole. Paroolid koosnevad kaheksast numbrimärgist. Veebisaidi turvaaukude tõttu lekkis ründajale teatavatel juhtudel andmesubjektide teave (nimi, perekonnanimi, sugu, sünniaeg ja -koht, maksukood, kasutaja tunnuskoodid), isegi kui kasutatud parool ei olnud õige või pangakonto ei olnud enam kasutuses. Rünne mõjutas ligikaudu 100 000 andmesubjekti. Ründajal õnnestus edukalt sisse logida neist ligikaudu 2 000 kontole, mille puhul kasutati ründaja katsetatud lihtparoole. Pärast ründe toimumist suutis vastutav töötleja tuvastada kõik ebaseaduslikud sisselogimiskatsed. Vastutav töötleja sai kinnitada, et pettusevastaste kontrollide kohaselt ei tehtud nendel kontodel ründe jooksul mingeid tehinguid. Pank oli andmetega seotud rikkumisest teadlik, sest tema turvaoperatsioonide keskus avastas hulgaliselt veebisaidile suunatud sisselogimistaotlusi. Vastusena blokeeris vastutav töötleja võimaluse veebisaidile sisse logida, lülitades sellise võimaluse välja, ja nõudis rikutud kontode paroolide lähtestamist. Vastutav töötleja teavitas rikkumisest ainult neid kasutajaid, kelle kontosid oli rikutud, see tähendab kasutajaid, kelle paroolid murti või kelle andmed avalikustati.

3.3.1 JUHTUM nr 7. Eelnevad meetmed ja riskihindamine

63. Oluline on märkida, et vastutavatel töötlejatel, kes käsitsevad äärmiselt isiklikku laadi andmeid,[21] on suurem vastutus tagada piisav andmeturve, näiteks peavad neil olema loodud turbekeskused ning kehtestatud muud intsidentide ennetamise, avastamise ja neile reageerimise meetmed. Kui need kõrgemad standardid ei ole täidetud, siis toob järelevalveasutuse uurimine tingimata kaasa rangemaid meetmeid.

64. Rikkumine on seotud finantsandmetega, mis lähevad kaugemale isikuandmetest ja kasutajatunnust käsitlevatest andmetest, seega on tegemist eriti tõsise rikkumisega. Mõjutatud isikute arv on suur.

[21] Näiteks teave andmesubjektide osutatud makseviiside kohta, nagu kaardinumbrid, pangakontod, elektroonilised maksed, palgaarvestus, pangakonto väljavõtted, majandusuuringud või mis tahes muud andmed, mille põhjal võib ilmneda andmesubjektidega seotud majanduslik teave.

65. Asjaolu, et sellises tundlikus keskkonnas võib aset leida rikkumine, osutab suurtele andmeturvaaukudele vastutava töötleja süsteemis ning võib näidata seda, millal mõjutatud meetmed on kooskõlas isikuandmete kaitse üldmääruse artikli 24 lõikega 1, artikli 25 lõikega 1 ja artikli 32 lõikega 1 vaja läbi vaadata ja neid ajakohastada. Rikutud andmed võimaldavad andmesubjekte kordumatult tuvastada ja sisaldavad nende kohta muud teavet (sealhulgas sugu ning sünniaeg ja -koht), lisaks saab ründaja neid kasutada klientide paroolide äraarvamiseks või panga klientide vastu suunatud harpuunimiskampaania läbiviimiseks.

66. Nendel põhjustel leiti, et tõenäoliselt tekitab andmetega seotud rikkumine suure riski asjaomaste andmesubjektide õigustele ja vabadustele[22]. Seepärast võib tulemuseks olla materiaalne (nt rahaline) ja mittemateriaalne kahju (nt identiteedivargus või pettus).

3.3.2 JUHTUM nr 7. Leevendamine ja kohustused

67. Vastutava töötleja võetud meetmed, mida juhtumi kirjelduses on mainitud, on piisavad. Rikkumise tagajärjel kõrvaldas ta ka veebisaidi nõrkused ja võttis muid meetmeid tulevikus sarnaste andmetega seotud rikkumiste vältimiseks, näiteks lisades asjaomasele veebisaidile kaksikautentimise ja minnes üle klientide tugevale autentimisele.

68. Sellise stsenaariumi puhul ei ole rikkumise dokumenteerimine vastavalt isikuandmete kaitse üldmääruse artikli 33 lõikele 5 ja rikkumisest järelevalveasutuse teavitamine vabatahtlik. Lisaks peaks vastutav töötleja kooskõlas isikuandmete kaitse üldmääruse artikliga 34 teavitama kõiki 100 000 andmesubjekti (sealhulgas andmesubjekte, kelle kontosid ei rikutud).

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

3.4 Korralduslikud ja tehnilised meetmed häkkerite rünnete mõju ennetamiseks/leevendamiseks

69. Samamoodi kui lunavararünnete puhul on vastutaval töötlejal sõltumata ründe tagajärgedest kohustus sarnaste juhtumite puhul IT-turvet uuesti hinnata.

70. Soovitatavad meetmed[23].

(*Alljärgnevate meetmete loetelu ei ole lõplik ega kõikehõlmav. Pigem on selle eesmärk anda ideid ennetamiseks ja võimalikeks lahendusteks. Iga töötlemistoiming on erinev, seega peab vastutav töötleja otsustama, millised meetmed on asjaomase olukorra puhul kõige sobilikumad.*)

- Tehnika tasemel krüpteerimine ja võtmete haldamine, eelkõige kui töödeldakse paroole ja tundlikke või finantsandmeid. Salastatud teabe (paroolid) krüptograafiline räsimine ja soolamine on alati eelistatavad paroolide krüpteerimisele. Eelistatav on kasutada autentimismeetodeid, millega välistatakse paroolide töötlemise vajadus serveri poolel.
- Süsteemi (tarkvara ja püsivara) ajakohasena hoidmine. Selle tagamine, et kehtestatud on kõik IT-turbemeetmed ja et need on tõhusad, ning nende korrapärane ajakohastamine töötlemise või asjaolude muutudes või arenedes. Selleks et tõendada vastavust isikuandmete kaitse üldmääruse artikli 5 lõike 1

[22] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

[23] Seoses turvaliste veebirakendustega vt ka https://www.owasp.org/index.php/Main_Page.

punktile f kooskõlas artikli 5 lõikega 2, peaks vastutav töötleja säilitama kõikide läbiviidud ajakohastuste andmed, sealhulgas andmed nende teostamise aja kohta.

- Tugeva autentimise meetodite, nagu kaksikautentimise ja autentimisserverite kasutamine, mida täiendab ajakohane paroolipoliitika.
- Turvalised arendusstandardid hõlmavad kasutajate sisendandmete filtreerimist (kasutades mõistlikkuse piires soovituslikke nimekirju), kasutajate sisendandmetest väljamurdu ja jõurünnete ennetamise meetmeid (nagu korduskatsete maksimaalse arvu piiramist). Selle tehnika tõhusal kasutamisel võib olla abi veebitulemüüridest.
- Kehtestatud on tugevad kasutajaprivileegid ja juurdepääsukontrolli haldamise põhimõtted.
- Sobilike, ajakohaste, tõhusate ja integreeritud tulemüüri-, sissetungi tuvastamise ja muude perimeetri kaitse süsteemide kasutamine.
- Süstemaatilised IT-turbe auditid ja nõrkuste hindamised (läbistustestimised).
- Korrapärased läbivaatamised ja testimised, mille eesmärk on tagada, et varukoopiaid saab kasutada kõikide selliste andmete taastamiseks, mille terviklust või kättesaadavust on mõjutatud.
- Seansi identifikaatori tavatekstina esitamata jätmine URLis.

4 ORGANISATSIOONISISESED INIMESTEGA SEOTUD RISKIALLIKAD

71. Rõhutada tuleb inimliku eksimuse rolli isikuandmetega seotud rikkumistes, sest seda esineb ulatuslikult. Kuna seda liiki rikkumised võivad olla nii tahtlikud kui ka tahtmatud, siis on vastutaval töötlejal väga keeruline nõrkusi kindlaks teha ja võtta meetmeid nende ennetamiseks. Andmekaitse ja eraelu puutumatuse eest vastutavate volinike rahvusvaheline konverents tunnistas selliste inimteguritega tegelemise tähtsust ja võttis 2019. aasta oktoobris vastu resolutsiooni, mis käsitleb inimlikku eksimust isikuandmetega seotud rikkumiste puhul[24]. Selles resolutsioonis juhitakse tähelepanu asjaolule, et inimliku eksimuse ennetamiseks peavad olema kehtestatud asjakohased kaitsemeetmed, ning esitatakse selliste kaitsemeetmete ja lähenemisviiside mitteammendav loetelu.

4.1 JUHTUM nr 8. Äriandmete varastamine töötaja poolt

Etteteatamisaja jooksul kopeerib ettevõtte töötaja ettevõtte andmebaasist äriandmeid. Töötajal on õigus pääseda andmetele juurde üksnes oma tööülesannete täitmiseks. Mitu kuud hiljem, pärast töölt lahkumist, kasutab ta sel viisil saadud andmeid (põhilised kontaktandmed) uue andmetöötluse jaoks, mille puhul tema on vastutav töötleja, eesmärgiga võtta ettevõtte klientidega ühendust, et meelitada nad oma uue ettevõtte klientideks.

4.1.1 JUHTUM nr 8. Eelnevad meetmed ja riskihindamine

72. Selle konkreetse juhtumi puhul ei võetud mingeid eelnevaid meetmeid, millega takistada töötajal ettevõtte klientide kontaktteabe kopeerimist, sest oma tööülesannete täitmiseks vajas ta õiguspärast juurdepääsu sellele teabele ja tal oli selline juurdepääs. Kuna enamiku kliendisuhete haldamist hõlmavate töökohtade puhul on töötajal vaja teatavat juurdepääsu isikuandmetele, võib selliseid rikkumisi olla kõige raskem ennetada. Juurdepääsupiirangud võivad piirata tööd, mida asjaomane töötaja suudab teha. Hästi läbimõeldud juurdepääsupõhimõtted ja pidev kontroll aitavad aga selliseid rikkumisi ennetada.

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

73. Nagu tavapäraselt, tuleb riskihindamisel arvesse võtta rikkumise liiki ning mõjutatud isikuandmete laadi, tundlikkust ja mahtu. Seda liiki rikkumiste puhul on tavaliselt tegemist konfidentsiaalsusega seotud rikkumisega, sest üldjuhul jäetakse andmebaas puutumatuks ja selle sisu „üksnes“ kopeeritakse edasiseks kasutamiseks. Ka mõjutatud andmete hulk on tavaliselt väike või keskmine. Selle konkreetse juhtumi puhul ei olnud mõjutatud mingid isikuandmete eriliigid, vaid töötaja vajas ainult klientide kontaktteavet, mis võimaldas tal nendega pärast ettevõttest lahkumist ühendust võtta. Seega ei olnud asjaomased andmed tundlikud.

74. Kuigi andmed pahatahtlikult kopeerinud endise töötaja ainus eesmärk võib piirduda ettevõtte klientide kontaktandmete hankimisega enda ärieesmärkidel, ei saa vastutav töötleja käsitada riski mõjutatud andmesubjektidele väikesena, sest vastutaval töötlejal puudub igasugune kindlustunne seoses töötaja kavatsustega. Rikkumise tagajärjed võivad küll piirduda soovimatu enesereklaami edastamisega endise töötaja poolt, ent välistatud ei ole varastatud andmete täiendav ja tõsisem kuritarvitamine, sõltuvalt endise töötaja läbiviidava töötlemise eesmärkidest[25].

4.1.2 JUHTUM nr 8. Leevendamine ja kohustused

75. Eespool kirjeldatud juhtumi puhul on rikkumise kahjulikku mõju keeruline leevendada. Selleks võib olla vaja võtta viivitamatuid õiguslikke meetmeid, et takistada endisel töötajal andmeid täiendavalt kuritarvitada ja levitada. Järgmise sammuna peaks olema eesmärk vältida tulevikus sarnaseid olukordi. Vastutav töötleja võib proovida nõuda endiselt töötajalt andmete kasutamise lõpetamist, kuid selle tegevuse tulemused on parimal juhul kaheldavad. Abiks võivad olla asjakohased tehnilised meetmed, nagu andmete irdseadmetesse kopeerimise või allalaadimise võimatuks muutmine.

76. Selliste juhtumite puhul ei ole olemas ühtset igasse olukorda sobivat lahendust, kuid süstemaatiline lähenemisviis võib aidata neid vältida. Näiteks võib ettevõte võimaluse korral kaaluda teatavate juurdepääsuvormide tühistamist töötajate puhul, kes on andnud märku sellest, et nad kavatsevad töölt lahkuda, või võtta kasutusele pääsulogid, et soovimatu juurdepääsu saaks logida ja märgistada. Töötajatega sõlmitud leping peaks sisaldama klausleid, millega selline tegevus keelatakse.

77. Kuna asjaomase rikkumisega ei kaasne suurt riski füüsiliste isikute õigustele ja vabadustele, piisab kokkuvõttes järelevalveasutuse teavitamisest. Vastutavale töötlejale võib aga olla kasulik ka andmesubjektide teavitamine, sest võib olla parem, kui nad kuulevad andmelekkest ettevõttelt, mitte endiselt töötajalt, kes püüab nendega ühendust võtta. Andmetega seotud rikkumise dokumenteerimine on õiguslik kohustus kooskõlas artikli 33 lõikega 5.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	X

[25] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

4.2 JUHTUM nr 9. Andmete juhuslik edastamine usaldusväärsele kolmandale isikule

Kindlustusagent märkas, et e-kirja kaudu saadud Exceli faili vigase seadistuse tõttu oli tal võimalik pääseda juurde kahe tosina kliendi teabele, kes ei kuulunud tema haldusalasse. Tema suhtes kehtib ametisaladuse hoidmise kohustus ja ta oli ainus isik, kes e-kirja sai. Vastutava töötleja ja kindlustusagendi suhtest tulenevalt on agent kohustatud isikuandmetega seotud rikkumisest vastutavale töötlejale viivitamata teatama. Seepärast teatas agent kohe veast vastutavale töötlejale, kes faili parandas ja selle uuesti välja saatis, paludes agendil eelmine sõnum kustutada. Eespool nimetatud korralduse kohaselt peab agent kustutamist kirjalikus avalduses kinnitama, mida ta ka tegi. Saadud teave ei hõlma isikuandmete eriliike, vaid ainult kontaktandmeid ja andmeid kindlustuse enda kohta (kindlustuse liik ja summa). Vastutav töötleja analüüsis rikkumisest mõjutatud andmeid ega teinud ei üksikisikute ega vastutava töötleja poolel kindlaks mingeid eripärasid, mis võiksid rikkumise mõju taset muuta.

4.2.1 JUHTUM nr 9. Eelnevad meetmed ja riskihindamine

78. Käesoleva juhtumi puhul ei tulene rikkumine töötaja tahtlikust tegevusest, vaid tähelepanematusest tingitud tahtmatust inimlikust eksimusest. Seda liiki rikkumisi saab ära hoida või nende sagedust vähendada a) koolitus-, haridus- ja teadlikkuse suurendamise programmide läbiviimisega, mille raames antakse töötajatele parem arusaamine isikuandmete kaitse tähtsusest, b) e-posti teel toimuva failide vahetamise vähendamisega, kasutades selle asemel näiteks sihtotstarbelisi kliendiandmete töötlemise süsteeme, c) failide topeltkontrollimisega enne nende saatmist ja d) failide koostamise ja saatmise eraldamisega.

79. Kõnealune andmetega seotud rikkumine puudutab üksnes andmete konfidentsiaalsust ega riku nende terviklust ja juurdepääsetavust. Andmetega seotud rikkumine puudutas vaid ligikaudu paari tosinat klienti, seega võib mõjutatud andmete hulka pidada väikesest. Peale selle ei sisalda mõjutatud isikuandmed tundlikke andmeid. Asjaolu, et volitatud töötleja võttis pärast andmetega seotud rikkumisest teadlikuks saamist viivitamata ühendust vastutava töötlejaga, võib pidada leevendavaks teguriks. (Samuti tuleb hinnata võimalust, et andmeid võidi saata ka teistele kindlustusagentidele, ja kui see kinnitust leiab, tuleb võtta nõuetekohaseid meetmeid.) Tänu pärast andmetega seotud rikkumist astutud asjakohastele sammudele ei ole sellel tõenäoliselt mingit mõju andmesubjektide õigustele ja vabadustele.

80. Kuna mõjutatud üksikisikute arv oli väike, rikkumine avastati kohe ja selle mõju minimeerimiseks võeti meetmeid, siis ei kujuta see konkreetne juhtum riski.

4.2.2 JUHTUM nr 9. Leevendamine ja kohustused

81. Samuti esineb teisi asjaolusid, mis riske maandavad: agendi suhtes kehtib ametisaladuse hoidmise kohustus, tema ise teatas probleemist vastutavale töötlejale ja taotluse põhjal kustutas ta faili. Teadlikkuse suurendamine ja võimaluse korral täiendavate sammude lisamine isikuandmeid sisaldavate dokumentide kontrollimisse aitavad tõenäoliselt sarnaseid juhtumeid tulevikus vältida.

82. Peale rikkumise dokumenteerimist kooskõlas artikli 33 lõikega 5 ei ole vaja muid meetmeid võtta.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

4.3 Korralduslikud ja tehnilised meetmed inimestega seotud organisatsioonisiseste riskiallikate mõju ennetamiseks/leevendamiseks

83. Allpool esitatud meetmete kombineerimine, mida kohaldatakse sõltuvalt iga juhtumi konkreetsetest tunnustest, peaks aitama vähendada sarnase rikkumise kordumise võimalust.

84. Soovitatavad meetmed.

(*Alljärgnevate meetmete loetelu ei ole lõplik ega kõikehõlmav. Pigem on selle eesmärk anda ideid ennetamiseks ja võimalikeks lahendusteks. Iga töötlemistoiming on erinev, seega peab vastutav töötleja otsustama, millised meetmed on asjaomase olukorra puhul kõige sobilikumad.*)

- Töötajate koolitus-, haridus- ja teadlikkuse suurendamise programmide korrapärane läbiviimine, mis käsitlevad nende kohustusi seoses privaatsuse ja turvalisusega ning isikuandmete turvalisusele esinevate ohtude avastamise ja neist teatamisega[26]. Teadlikkuse suurendamise programmi väljatöötamine, et tuletada töötajatele meelde kõige levinumaid eksimusi, mille tulemuseks on andmetega seotud rikkumised, ja seda, kuidas neid vältida.
- Usaldusväärsete ja tõhusate andmekaitse- ja privaatsuse tagamise tavade, menetluste ja süsteemide kehtestamine[27].
- Privaatsuse tagamise tavade, menetluste ja süsteemide hindamine nende jätkuva tõhususe tagamiseks[28].
- Nõuetekohaste juurdepääsukontrolli põhimõtete koostamine ja kasutajatelt eeskirjadest kinnipidamise nõudmine.
- Tundlikele isikuandmetele juurdepääsemisel kasutaja autentimise nõudmise tehnikate rakendamine.
- Kasutaja ettevõttega seotud konto blokeerimine niipea, kui isik ettevõttest lahkub.
- Failiserveri ja töötajate tööjaamade vaheliste ebaharilike andmevoogude kontrollimine.
- Sisendi-väljundi liidese turvalisuse tagamine BIOSis või tarkvara kasutamise kaudu, millega kontrollitakse arvutiliideste kasutamist (nt USB/CD/DVD jne lukustamine või avamine).
- Töötajate juurdepääsupoliitika läbivaatamine (nt tundlikele andmetele juurdepääsemise logimine ja kasutajalt ärilise põhjuse sisestamise nõudmine, et sellega saaks auditi käigus tutvuda).
- Avatud pilvteenuste blokeerimine.
- Teadaolevatele avatud postiteenustele juurdepääsu keelamine ja takistamine.
- Operatsioonisüsteemis ekraanipildi printimise blokeerimine.
- Puhta töölaua põhimõtte järgimise tagamine.
- Kõikide arvutite automaatne lukustamine pärast teatavat tegevusetusaega.
- Mehhanismide (nt (traadita) läbipääsuload lukustatud kontodele sisselogimiseks / nende avamiseks) kasutamine kasutajate kiireks vahetamiseks jagatud keskkondades.
- Isikuandmete haldamiseks sihtotstarbeliste süsteemide kasutamine, milles rakendatakse nõuetekohaseid juurdepääsukontrolli mehhanisme ja mis ennetavad inimlikku eksimust, nagu teadete saatmist valele adressaadile. Arvutustabelite ja muude kontoridokumentide kasutamine ei ole nõuetekohane viis kliendiandmete haldamiseks.

5 KAOTATUD VÕI VARASTATUD SEADMED JA PABERKANDJAL DOKUMENDID

85. Sageli tuleb ette kaasaskantavate seadete kaotamist või varastamist. Sellistel juhtudel peab vastutav töötleja võtma arvesse töötlemistoimingu asjaolusid, nagu seadmele salvestatud andmete liiki, samuti toetavaid

[26] Isikuandmetega seotud rikkumiste puhul inimlikku eksimust käsitleva resolutsiooni 2. punkti alapunkt i.

[27] Isikuandmetega seotud rikkumiste puhul inimlikku eksimust käsitleva resolutsiooni 2. punkti alapunkt ii.

[28] Isikuandmetega seotud rikkumiste puhul inimlikku eksimust käsitleva resolutsiooni 2. punkti alapunkt iii.

varasid ja enne rikkumist asjakohase turvataseme tagamiseks võetud meetmeid. Kõik need elemendid mõjutavad andmetega seotud rikkumise võimalikku mõju. Riskihindamine võib olla keeruline, sest seade ei ole enam kättesaadav.

86. Seda liiki rikkumised saab alati liigitada konfidentsiaalsusega seotud rikkumiseks. Kui aga varastatud andmebaasist ei ole tehtud varukoopiat, siis võib rikkumise liik olla seotud ka tervikluse ja kättesaadavusega.

87. Alljärgnevad stsenaariumid illustreerivad, kuidas eespool nimetatud asjaolud mõjutavad andmetega seotud rikkumise tõenäosust ja tõsidust.

5.1 JUHTUM nr 10. Varastatud materjal, kuhu on salvestatud krüpteeritud isikuandmed

Laste päevakeskusesse sissemurdmise käigus varastati kaks tahvelarvutit. Tahvelarvutid sisaldasid rakendust, kus hoiti päevakeskuses käivate laste isikuandmeid. Tegemist oli laste nimede, sünnikuupäevade ja haridusalaste isikuandmetega. Nii krüpteeritud tahvelarvutid, mis olid sissemurdmise ajal välja lülitatud, kui ka rakendus olid kaitstud tugeva parooliga. Varundatud andmed olid vastutavale töötlejale tõhusalt ja kiirelt kättesaadavad. Pärast sissemurdmisest teadasaamist andis päevakeskus varsti pärast sissemurdmise avastamist kaugkäsu tahvelarvutite sisu kustutamiseks.

5.1.1 JUHTUM nr 10. Eelnevad meetmed ja riskihindamine

88. Selle konkreetse juhtumi puhul võttis vastutav töötleja andmetega seotud võimaliku rikkumise ennetamiseks ja selle mõju leevendamiseks piisavaid meetmeid, kasutades seadmete krüpteerimist, kehtestades piisava paroolikaitse ja tagades tahvelarvutites salvestatud andmete varundamise. (Soovitatavate meetmete loetelu on esitatud punktis 5.7.)

89. Pärast rikkumisest teadlikuks saamist peaks vastutav töötleja hindama riski allikat, andmetöötlust toetavaid süsteeme, asjaomaste isikuandmete liiki ja andmetega seotud rikkumise võimalikku mõju seotud üksikisikutele. Eespool kirjeldatud andmetega seotud rikkumine oleks puudutanud asjaomaste andmete konfidentsiaalsust, kättesaadavust ja terviklust, ent tänu vastutava töötleja asjakohastele menetlustele enne ja pärast andmetega seotud rikkumist ei leidnud aset ükski neist rikkumistest.

5.1.2 JUHTUM nr 10. Leevendamine ja kohustused

90. Seadmetes sisalduvate andmete konfidentsiaalsust ei rikutud tänu nii tahvelarvutite kui ka rakenduste tugeva parooliga kaitsmisele. Tahvelarvutid olid seadistatud nii, et parooli kehtestamine tähendas ühtlasi seadmes sisalduvate andmete krüpteerimist. See oli veelgi tõhusam tänu vastutava töötleja tegevusele, kes püüdis kogu varastatud seadmetes sisalduva teabe kaugkustutada.

91. Võetud meetmete tulemusel säilitati ka andmete konfidentsiaalsus. Peale selle tagati varukoopiaga isikuandmete jätkuv kättesaadavus, seega ei oleks saanud tekkida võimalikku kahjulikku mõju.

92. Nende asjaolude tõttu ei olnud tõenäoline, et eespool kirjeldatud andmetega seotud rikkumise tulemusel oleks tekkinud risk andmesubjektide õigustele ja vabadustele, seega ei olnud vaja järelevalveasutust ega asjaomaseid andmesubjekte teavitada. Küll aga tuleb ka see andmetega seotud rikkumine kooskõlas artikli 33 lõikega 5 dokumenteerida.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

5.2 JUHTUM nr 11. Varastatud materjal, kuhu on salvestatud krüpteerimata isikuandmed

Varastati teenuseosutaja töötaja elektrooniline sülearvuti. Varastatud sülearvuti sisaldas enam kui 100 000 kliendi nimesid, perekonnanimesid, sugu, aadresse ja sünnikuupäevi. Kuna varastatud seade ei olnud kättesaadav, siis ei olnud võimalik kindlaks teha, kas mõjutati ka muid isikuandmete liike. Juurdepääs sülearvuti kõvakettale ei olnud parooliga kaitstud. Isikuandmeid oli võimalik taastada kättesaadavate igapäevaste varukoopiate põhjal.

5.2.1 JUHTUM nr 11. Eelnevad meetmed ja riskihindamine

93. Vastutav töötleja ei olnud võtnud eelnevaid turvameetmeid ja seega olid varastatud sülearvutis salvestatud isikuandmed vargale või mis tahes teisele isikule, kes seadme järgnevalt oma valdusesse sai, hõlpsalt juurdepääsetavad.

94. See andmetega seotud rikkumine puudutab varastatud seadmel salvestatud andmete konfidentsiaalsust.

95. Käesoleval juhul oli isikuandmeid sisaldav sülearvuti haavatav, sest see ei olnud parooliga kaitstud ega krüpteeritud. Põhiliste turvameetmete puudumine tõstab mõjutatud andmesubjektidele avalduva riski taset. Peale selle on probleemne ka asjaomaste andmesubjektide tuvastamine, mis samuti suurendab rikkumise tõsidust. Riski suurendab asjaomaste üksikisikute märkimisväärne arv, sellest hoolimata ei puudutanud andmetega seotud rikkumine isikuandmete eriliike.

96. Riskihindamise käigus[29] peaks vastutav töötleja võtma arvesse konfidentsiaalsusega seotud rikkumise võimalikke tagajärgi ja võimalikku kahjulikku mõju. Rikkumise tulemusel võivad asjaomased andmesubjektid langeda varastatud seadmes kättesaadavatel andmetel põhineva identiteedivarguse ohvriks, seega peetakse riski suureks.

5.2.2 JUHTUM nr 11. Leevendamine ja kohustused

97. Seadme krüpteerimise sisselülitamine ja salvestatud andmebaasi tugeva parooliga kaitsmine oleksid välistanud olukorra, kus andmetega seotud rikkumise tulemusel tekib risk andmesubjektide õigustele ja vabadustele.

98. Nende asjaolude tõttu on nõutav järelevalveasutuse teavitamine, samuti on vaja teavitada asjaomaseid andmesubjekte.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

5.3 JUHTUM nr 12. Tundlikke andmeid sisaldavad varastatud paberkandjal failid

Uimastisõltlaste rehabilitatsioonikeskusest varastati paberkandjal logiraamat. Raamat sisaldas rehabilitatsioonikeskusesse vastu võetud patsientide põhilisi isiku- ja terviseandmeid. Andmeid säilitati ainult paberkandjal ja patsiente ravivatele arstidele ei olnud kättesaadavad varukoopiad. Raamatut ei hoitud lukustatud sahtlis ega ruumis ning vastutav töötleja ei olnud kehtestanud ei juurdepääsukontrolli süsteemi ega mingit muud paberkandjal dokumentide turvameedet.

[29] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

5.3.1 JUHTUM nr 12. Eelnevad meetmed ja riskihindamine

99. Vastutav töötleja ei olnud võtnud eelnevaid turvameetmeid ja seega olid raamatus säilitatavad isikuandmed selle leidnud isikule hõlpsalt juurdepääsetavad. Peale selle tähendab raamatus säilitatavate isikuandmete laad, et varundatud andmete puudumine kujutab endast väga tõsist riskitegurit.

100. Käesolev juhtum on näide andmetega seotud suure riskiga rikkumisest. Asjakohaste turvaalaste ettevaatusabinõude puudumise tõttu läksid kaduma tundlikud terviseandmed vastavalt isikuandmete kaitse üldmääruse artikli 9 lõikele 1. Kuna käesoleva juhtumi puhul oli tegemist isikuandmete eriliigiga, siis kasvas võimalik risk asjaomastele andmesubjektidele, mida riski hindav vastutav töötleja peab samuti arvesse võtma[30].

101. See rikkumine on seotud asjaomaste isikuandmete konfidentsiaalsuse, kättesaadavuse ja terviklusega. Rikkumise tulemusel rikuti arstisaladust ja loata kolmandad isikud võivad saada juurdepääsu patsientide privaatsele meditsiiniteabele, millel võib olla tõsine mõju patsientide eraelule. Kättesaadavusega seotud rikkumine võib häirida ka patsientide ravi jätkamist. Kuna ei saa välistada raamatu sisu teatavate osade muutmist/kustutamist, siis on rikutud ka isikuandmete terviklust.

5.3.2 JUHTUM nr 12. Leevendamine ja kohustused

102. Kaitsemeetmete hindamisel tuleb võtta arvesse toetava vara liiki. Kuna patsientide logiraamatu näol on tegemist füüsilise dokumendiga, siis oleks selle kaitsmine pidanud olema korraldatud erinevalt kui elektroonilise seadme puhul. Andmetega seotud rikkumise oleksid võinud ära hoida patsientide nimede pseudonümiseerimine, raamatu hoidmine kaitstud asukohas ja lukustatud sahtlis või ruumis ning nõuetekohane juurdepääsukontroll koos autentimisega logiraamatule juurdepääsemisel.

103. Eespool kirjeldatud andmetega seotud rikkumine võib asjaomaseid andmesubjekte tõsiselt mõjutada, seega on järelevalveasutuse ja asjaomaste andmesubjektide teavitamine kohustuslik.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

5.4 Korralduslikud ja tehnilised meetmed seadmete kaotamise või varguse mõju ennetamiseks/leevendamiseks

104. Allpool esitatud meetmete kombineerimine, mida kohaldatakse sõltuvalt iga juhtumi konkreetsetest tunnustest, peaks aitama vähendada sarnase rikkumise kordumise võimalust.

105. Soovitatavad meetmed.

(*Alljärgnevate meetmete loetelu ei ole lõplik ega kõikehõlmav. Pigem on selle eesmärk anda ideid ennetamiseks ja võimalikeks lahendusteks. Iga töötlemistoiming on erinev, seega peab vastutav töötleja otsustama, millised meetmed on asjaomase olukorra puhul kõige sobilikumad.*)

- Seadme krüpteerimise sisselülitamine (nagu Bitlocker, Veracrypt või DM-Crypt).
- Kõikidel seadmetel pääsukoodide/paroolide kasutamine. Kõikide kaasaskantavate elektrooniliste seadmete krüpteerimine viisil, mille puhul on dekrüpteerimiseks vaja sisestada keeruline parool.
- Mitmikautentimise kasutamine.

[30] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

- Hõlpsalt kaasaskantavate seadmete selliste funktsioonide sisselülitamine, mis võimaldavad need kaotsimineku või valesse kohta asetamise korral üles leida.
- Kaasaskantavate seadmete haldamise tarkvara/rakenduse ja asukohatuvastuse kasutamine. Pimestustõrjefiltrite kasutamine. Kõikide järelevalveta seadmete sulgemine.
- Kui see on võimalik ja asjaomase andmetöötluse puhul asjakohane, siis isikuandmete salvestamine mitte kaasaskantavas seadmes, vaid keskses põhiserveris.
- Kui tööjaam on ühendatud ettevõtte kohtvõrguga, siis töökaustade põhjal automaatsete varukoopiate tegemine, kui isikuandmete säilitamine nendes kaustades on vältimatu.
- Turvalise virtuaalse privaatvõrgu kasutamine (nt sellise võrgu, mille puhul nõutakse turvalise ühenduse loomiseks eraldi kaksikautentimisvõtit) kaasaskantavate seadmete põhiserveriga ühendamiseks.
- Töötajate varustamine füüsiliste lukkudega, et neil oleks võimalik tagada järelevalveta kaasaskantavate seadmete füüsiline turvalisus.
- Seadmete väljaspool ettevõtet kasutamise nõuetekohane reguleerimine.
- Seadmete ettevõttesisese kasutamise nõuetekohane reguleerimine.
- Kaasaskantavate seadmete haldamise tarkvara/rakenduse kasutamine ja kaugkustutusfunktsiooni võimaldamine.
- Seadmete keskse haldamise kasutamine, mille puhul lõppkasutajatel on minimaalsed tarkvara paigaldamise õigused.
- Füüsiliste juurdepääsukontrollide paigaldamine.
- Tundliku teabe kaasaskantavates seadmetes või kõvaketastel säilitamise vältimine. Kui vaja on juurdepääsu ettevõtte sisesüsteemile, tuleks kasutada eespool nimetatud turvalisi kanaleid.

6 EKSLIK POSTITAMINE

106. Ka sellel juhul on riski allikas organisatsioonisisene inimlik eksimus, kuid siinkohal ei tulene rikkumine pahatahtlikust tegevusest. Selle põhjuseks on tähelepanematus. Vastutaval töötlejal ei ole palju võimalusi pärast rikkumise toimumist midagi ette võtta, seega on ennetamine selliste juhtumite korral veelgi olulisem kui muude rikkumise liikide puhul.

6.1 JUHTUM nr 13. Posti teel saadetud kirjaga seotud eksimus

Jaemüüja pakendas kaks kingatellimust. Inimliku eksimuse tõttu läksid kaks pakendamisarvet vahetusse, mille tulemusel mõlemad tooted ja vastavad pakendamisarved saadeti valele isikule. See tähendab, et kaks klienti said kätte teineteise tellimuse, sealhulgas isikuandmeid sisaldavad pakendamisarved. Pärast rikkumisest teadlikuks saamist kutsus vastutav töötleja tellimused tagasi ja saatis need õigetele adressaatidele.

6.1.1 JUHTUM nr 13. Eelnevad meetmed ja riskihindamine

107. Arved sisaldasid edukaks kättetoimetamiseks vajalikke isikuandmeid (nimi, aadress ning ostetud artikkel ja selle hind). Oluline on kindlaks teha, kuidas sai inimlik eksimus üldse juhtuda ja kas seda oleks olnud mingil viisil võimalik ära hoida. Konkreetse kirjeldatud juhtumi puhul on risk väike, sest tegemist ei ole isikuandmete eriliikidega ega muude andmetega, mille kuritarvitamisega võib kaasneda suurem kahjulik mõju, rikkumine ei ole tingitud vastutava töötleja süstemaatilisest veast ja see puudutab ainult kahte isikut. Tuvastada ei saa kahjulikku mõju üksikisikutele.

6.1.2 JUHTUM nr 13. Leevendamine ja kohustused

108. Vastutav töötleja peaks korraldama artiklite ja nendega kaasas olnud arvete tasuta tagastamise ning samuti paluma valedel adressaatidel hävitada/kustutada kõik teise isiku isikuandmeid sisaldavate arvete võimalikud koopiad.

109. Isegi kui rikkumise endaga ei kaasne suurt riski mõjutatud üksikisikute õigustele ja vabadustele ning seega ei nõuta isikuandmete kaitse üldmääruse artikli 34 alusel andmesubjektide teavitamist, ei saa neile rikkumisest teatamist vältida, sest riski maandamiseks on vaja nende koostööd.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

6.2 JUHTUM nr 14. Kirja teel eksikombel saadetud äärmiselt konfidentsiaalsed isikuandmed

Avaliku haldusasutuse tööhõive osakond saatis oma süsteemis tööotsijatena registreeritud isikutele e-kirja teel sõnumi tulevaste koolituste kohta. Eksimuse tõttu oli sellele e-kirjale manustatud dokument, mis sisaldas kõikide kõnealuste tööotsijate isikuandmeid (nimi, e-posti aadress, postiaadress, sotsiaalkindlustusnumber). Mõjutatud isikute arv on üle 60 000. Järgnevalt võttis asutus kõikide kirja saajatega ühendust ning palus neil eelmise sõnumi kustutada ja selles sisalduvat teavet mitte kasutada.

6.2.1 JUHTUM nr 14. Eelnevad meetmed ja riskihindamine

110. Selliste sõnumite saatmise suhtes oleks tulnud rakendada rangemaid eeskirju. Kaaluda tuleb täiendavate kontrollimehhanismide rakendamist.

111. Mõjutatud isikute arv on märkimisväärne ja asjaolu, et lisaks elementaarsematele isikuandmetele oli tegemist ka nende isikute sotsiaalkindlustusnumbritega, suurendab veelgi riski, mida võib pidada suureks[31]. Vastutav töötleja ei saa takistada seda, et mõni kirja saaja andmeid lõppkokkuvõttes levitab.

6.2.2 JUHTUM nr 14. Leevendamine ja kohustused

112. Nagu eespool märgitud, on võimalused sarnase rikkumisega kaasnevate riskide maandamiseks piiratud. Kuigi vastutav töötleja palus sõnumi kustutada, ei saa ta sundida kirja saajaid seda tegema ning selle tulemusel ei saa ta olla kindel, et nad palve täidavad.

113. Selliste juhtumite puhul peaks olema iseenesest mõistetav, et võtta tuleb kõik kolm allpool osutatud meedet.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

6.3 JUHTUM nr 15. Kirja teel eksikombel saadetud isikuandmed

[31] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

Hotellis viie päeva jooksul toimuva inglise õiguskeele kursuse osalejate nimekiri saadeti hotelli asemel eksikombel 15-le kursusel eelnevalt osalenud isikule. Nimekiri sisaldas 15 osaleja nimesid, e-posti aadresse ja toitumiseelistusi. Toitumiseelistuse andmed olid esitanud ainult kaks osalejat, märkides, et neil on laktoositalumatus. Ühegi osaleja identiteet ei ole kaitstud. Vastutav töötleja avastab eksimuse vahetult pärast nimekirja saatmist ning teavitab sellest kirja saajaid ja palub neil nimekirja kustutada.

6.3.1 JUHTUM nr 15. Eelnevad meetmed ja riskihindamine

114. Isikuandmeid sisaldavate sõnumite saatmise suhtes oleks tulnud rakendada rangeid eeskirju. Kaaluda tuleb täiendavate kontrollimehhanismide rakendamist.

115. Isikuandmete laadist, tundlikkusest, mahust ja kontekstist tulenevad riskid on väikesed. Isikuandmed hõlmavad tundlikke andmeid kahe osaleja toidueelistuste kohta. Isegi kui kellegi laktoositalumatust käsitleva teabe näol on tegemist terviseandmetega, siis tuleks riski, et neid andmeid kasutatakse kahjustaval viisil, pidada suhteliselt väikeseks. Kuigi tervist käsitlevate andmete korral üldjuhul eeldatakse, et rikkumisega kaasneb andmesubjektile suur risk,[32] siis samas ei saa selle konkreetse juhtumi puhul teha kindlaks riski, et rikkumine tekitaks laktoositalumatust käsitleva teabe loata avalikustamise tõttu andmesubjektile füüsilist, materiaalset või mittemateriaalset kahju. Vastupidiselt teatavatele muudele toidueelistustele ei saa laktoositalumatust tavaliselt seostada mingite religioossete ega filosoofiliste tõekspidamistega. Ka rikutud andmete hulk ja mõjutatud andmesubjektide arv on väga väike.

6.3.2 JUHTUM nr 15. Leevendamine ja kohustused

116. Kokkuvõttes võib märkida, et rikkumine ei avaldanud andmesubjektidele olulist mõju. Asjaolu, et vastutav töötleja võttis pärast eksimusest teadlikuks saamist viivitamata ühendust kirja saajatega, võib pidada leevendavaks teguriks.

117. E-kirja valele/loata adressaadile saatmise korral soovitatakse vastutaval töötlejal saata tahtmatutele adressaatidele pimekoopiana täiendav kiri, milles esitatakse vabandus, palutakse rikkumisega seotud e-kiri kustutada ja teavitatakse adressaate asjaolust, et neil ei ole õigust neile teatavaks saanud e-posti aadresse edaspidi kasutada.

118. Nende asjaolude tõttu ei olnud tõenäoline, et selle andmetega seotud rikkumise tulemusel oleks tekkinud risk andmesubjektide õigustele ja vabadustele, seega ei olnud vaja järelevalveasutust ega asjaomaseid andmesubjekte teavitada. Küll aga tuleb ka see andmetega seotud rikkumine kooskõlas artikli 33 lõikega 5 dokumenteerida.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	X	X

6.4 JUHTUM nr 16. Posti teel saadetud kirjaga seotud eksimus

[32] Vt suunised WP250, lk 23.

Kindlustusgrupp pakub autokindlustust. Selleks saadab ta posti teel välja regulaarselt kohandatud kindlustusmaksete lepinguid. Lisaks kindlustusvõtja nimele ja aadressile sisaldab kiri sõiduki registreerimisnumbrit, mille numbrimärgid ei ole varjatud, jooksva ja järgmise kindlustusaasta kindlustusmäärasid, keskmist aastast läbisõitu ja kindlustusvõtja sünnikuupäeva. Need andmed ei hõlma isikuandmete kaitse üldmääruse artikli 9 kohaseid terviseandmeid, makseandmeid (pangaandmeid), majanduslikke ega finantsandmeid.

Kirjad pannakse ümbrikutesse automatiseeritud masinatega. Mehaanilise vea tõttu pannakse kaks kirja eri kindlustusvõtjatele ühte ümbrikusse ja saadetakse posti teel ühele kindlustusvõtjale. See kindlusvõtja avab kirja kodus ja tutvub nii talle õigesti kättetoimetatud kirja kui ka eksikombel kättetoimetatud teist kindlustusvõtjat käsitleva kirjaga.

6.4.1 JUHTUM nr 16. Eelnevad meetmed ja riskihindamine

119. Eksikombel kättetoimetatud kiri sisaldab nime, aadressi, sünnikuupäeva, sõiduki varjamatut registreerimisnumbrit ning jooksva ja järgmise aasta kindlustusmäära liigitust. Mõjutatud isikule avalduvat mõju tuleb käsitada keskmisena, sest loata adressaadile avalikustati teavet, mis ei ole avalikult kättesaadav, nagu sünnikuupäev või sõiduki varjamatud registreerimisnumbrid ja üksikasjalikud andmed kindlustusmäärade muutuse kohta. Nende andmete väärkasutamise tõenäosust hinnatakse väikeseks kuni keskmiseks. Kuigi paljud adressaadid eksikombel saadud kirja tõenäoliselt ära viskavad, ei saa aga üksikjuhtumite puhul täielikult välistada võimalust, et kiri pannakse üles sotsiaalvõrgustikesse või et kindlustusvõtjaga võetakse ühendust.

6.4.2 JUHTUM nr 16. Leevendamine ja kohustused

120. Vastutav töötleja peaks laskma oma kuludega originaaldokumendi tagasi saata. Samuti tuleks vale adressaati teavitada sellest, et ta ei tohi loetud teavet kuritarvitada.

121. Masspostituse korral, milleks kasutatakse täisautomatiseeritud masinaid, ei ole tõenäoliselt kunagi täielikult võimalik vältida vigu posti kättetoimetamisel. Postitamise suurema sageduse puhul on aga vaja kontrollida, kas kirju ümbrikusse panevad masinad on piisavalt õigesti seadistatud ja hooldatud või kas selline rikkumine võib tuleneda mõnest muust süsteemsest probleemist.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	X

6.5 Korralduslikud ja tehnilised meetmed eksliku postitamise mõju ennetamiseks/leevendamiseks

122. Allpool esitatud meetmete kombineerimine, mida kohaldatakse sõltuvalt iga juhtumi konkreetsetest tunnustest, peaks aitama vähendada sarnase rikkumise kordumise võimalust.

123. Soovitatavad meetmed.

(*Alljärgnevate meetmete loetelu ei ole lõplik ega kõikehõlmav. Pigem on selle eesmärk anda ideid ennetamiseks ja võimalikeks lahendusteks. Iga töötlemistoiming on erinev, seega peab vastutav töötleja otsustama, millised meetmed on asjaomase olukorra puhul kõige sobilikumad.*)

- Kirjade/e-kirjade saatmise kohta täpsete normide kehtestamine, mida ei saa mitmeti tõlgendada.
- Töötajate piisav koolitamine kirjade/e-kirjade saatmise alal.
- Mitmele adressaadile e-kirja saatmisel nende vaikimisi loetlemine pimekoopia väljal.
- Kui e-kirju saadetakse mitmele adressaadile ja nad ei ole pimekoopia väljal loetletud, tuleb nõuda lisakinnitust.

- Nelja silma põhimõtte rakendamine.
- Aadresside automaatne sisestamine, mitte käsitsi kirjutamine, võttes need kättesaadavast ja ajakohasest andmebaasist; aadresside automaatse sisestamise süsteem tuleb korrapäraselt läbi vaadata eesmärgiga kontrollida, et see ei sisalda peidetud vigu ega valesid sätteid.
- Sõnumite saatmisel viivituste rakendamine (nt saab sõnumi pärast saatmisnupule klikkimist teatava aja jooksul kustutada / seda redigeerida).
- E-kirja aadresside trükkimisel automaattäitmise väljalülitamine.
- Teadlikkuse suurendamise kursused kõige levinumate vigade kohta, mille tulemuseks on isikuandmetega seotud rikkumine.
- Koolituskursused ja käsiraamatud selle kohta, kuidas tulla toime intsidentidega, mille tulemuseks on isikuandmetega seotud rikkumine, ja keda neist teavitada (andmekaitseametniku kaasamine).

7 MUUD JUHTUMID – SOTSIAALNE MANIPULATSIOON

7.1 JUHTUM nr 17. Identiteedivargus

Telekommunikatsioonіettevõte kõnekeskusesse helistab isik, kes esitleb end kliendina. Väidetav klient nõuab ettevõttelt selle e-posti aadressi muutmist, kuhu arveldusteave tuleks edaspidi saata. Kõnekeskuse töötaja valideerib kliendi isiku, küsides teatavaid ettevõtte menetlustes määratletud isikuandmeid. Helistaja nimetab õigesti kliendi maksukohustuslase numbri ja postiaadressi (sest tal oli nendele andmetele juurdepääs). Pärast tema isiku valideerimist teeb operaator taotletud muudatuse ja edaspidi saadetakse arvetega seotud teave uuele e-posti aadressile. Menetluse raames ei ole ette nähtud teate saatmist eelmisele e-posti aadressile. Järgmisel kuul võtab ettevõttega ühendust õiguspärane klient ja küsib, miks ta ei saa arveid oma e-posti aadressile, ning eitab helistamist ja oma e-posti aadressi muutmise nõudmist. Hiljem mõistab ettevõte, et see teave on saadetud ebaseaduslikule kasutajale ja pöörab muudatuse tagasi.

7.1.1 JUHTUM nr 17. Riskihindamine, leevendamine ja kohustused

124. See juhtum näitlikustab eelnevate meetmete tähtsust. Riskide seisukohast on rikkumisega kaasneva riski tase kõrge,33 sest arveldusandmed võivad anda teavet andmesubjekti eraelu (nt harjumuste, kontaktide) kohta ja tekitada olulist kahju (nt ahistav jälitamine, risk kehalisele puutumatusele). Samuti võib ründe jooksul saadud isikuandmeid kasutada konto ülevõtmise hõlbustamiseks selles organisatsioonis või muude autentimismeetmete ärakasutamiseks teistes organisatsioonides. Neid riske arvesse võttes peaks nõuetekohane autentimismeede vastama kõrgetele normidele, sõltuvalt sellest, milliseid isikuandmeid saab autentimise tulemusel töödelda.

125. Selle tulemusel peab vastutav töötleja teavitama nii järelevalveasutust kui ka andmesubjekti.

[33] Seoses suunistega töötlemistoimingute kohta, mille tulemusena „*tekib tõenäoliselt suur oht*“, vt joonealune märkus nr 10 eespool.

126. Kõnealuse juhtumi puhul tuleb ilmselgelt täiustada varasemat klientide isiku valideerimise protsessi. Autentimiseks kasutatud meetodid ei olnud piisavad. Pahatahtlik isik suutis teeselda, et ta on ettenähtud kasutaja, kasutades avalikult kättesaadavat teavet ja teavet, millele tal oli muul viisil juurdepääs.

127. Seda liiki staatilise teadmistepõhise autentimise (mille puhul vastus ei muutu ja teave ei ole salajane, nagu see on seda parooli korral) kasutamine ei ole soovitatav.

128. Selle asemel peaks ettevõte kasutama sellist autentimisvormi, mis tagab kõrgetasemelise kindlustunde, et autenditud kasutaja on ettenähtud isik, mitte keegi teine. Probleemi lahendaks lisakanaliga mitmikautentimise meetodi kasutusevõtmine, näiteks et muudatuse nõudmist kontrollida, saates kinnitustaotluse eelmisel aadressil, või täiendavate küsimuste lisamine ja sellise teabe küsimine, mis on nähtav ainult eelmistel arvetel. Vastutava töötleja kohustus on otsustada, milliseid meetmeid kehtestada, sest tema tunneb oma ettevõttesiseste toimingute üksikasju ja nõudeid kõige paremini.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓

7.2 JUHTUM nr 18. E-kirjadega seotud andmeleke

Hüpermarketite kett avastas kolm kuud pärast teatavate e-posti kontode konfigureerimist, et neid kontosid oli muudetud ja kehtestatud reeglid, mille kohaselt iga kindlaid väljendeid (nt „arve“, „makse“, „pangaülekanne“, „krediitkaardi autentimine“, „pangakonto andmed“) sisaldav e-kiri paigutatakse kasutamata kausta ja samuti edastatakse välisele e-posti aadressile. Selleks ajaks oli juba läbi viidud ka sotsiaalse manipulatsiooni rünne, see tähendab tarnijana esinenud ründaja oli muutnud tarnija pangakonto andmed enda andmeteks. Samuti oli selleks ajaks saadetud mitu uue pangakonto andmeid sisaldavat võltsarvet. E-posti platvormi jälgimissüsteem andis kaustade kohta hoiatuse. Ettevõte ei suutnud tuvastada, kuidas ründaja üldse sai juurdepääsu e-posti kontodele, kuid eeldas, et selles oli süüdi nakatatud fail, mis andis juurdepääsu maksete eest vastutavate kasutajate rühmale.

E-kirjade märksõnadel põhineva edastamise tõttu sai ründaja teavet 99 töötaja kohta: nime ja konkreetse kuu palka käsitleva teabe 89 andesubjekti kohta ning nime, perekonnaseisu, laste arvu, palka, töötunde ja ülejäänud palga saamist käsitleva teabe kümne töötaja kohta, kelle tööleping oli lõpetatud. Vastutav töötleja teavitas üksnes kümmet viimasesse rühma kuuluvat töötajat.

7.2.1 JUHTUM nr 18. Riskihindamine, leevendamine ja kohustused

129. Isegi kui ründaja eesmärk tõenäoliselt ei olnud isikuandmete kogumine, siis kuna rikkumisega võib kaasneda nii materiaalne (nt rahaline) kui ka mittemateriaalne kahju (nt identiteedivargus või pettus) või kuna andmeid saab kasutada muude rünnete hõlbustamiseks (nt andmepüügiks), tekitab isikuandmetega seotud rikkumine tõenäoliselt suure riski füüsiliste isikute õigustele ja vabadustele. Seepärast tuleks rikkumisest teatada kõigile 99 töötajale, mitte ainult neile kümnele töötajale, kelle palgateave lekkis.

130. Pärast rikkumisest teada saamist nõudis vastutav töötleja rikutud kontode paroolide muutmist, blokeeris e-kirjade saatmise ründaja e-posti kontole, teavitas ründaja kasutatud e-posti pakkuvat teenuseosutajat ründaja tegevusest, eemaldas ründaja kehtestatud eeskirjad ja täiustas jälgimissüsteemi antavaid hoiatusi, et hoiatus antaks niipea, kui automaatne eeskiri luuakse. Teise võimalusena võib vastutav töötleja kõrvaldada kasutajate õiguse määrata edastamiseeskirju, millisel juhul saab seda teha IT-teenuste meeskond ainult

taotluse korral, või kehtestada põhimõtte, et finantsandmete käsitlemise valdkondades peavad kasutajad korra nädalas või tihedamini kontrollima nende kontodel määratud eeskirju ja neist teavitama.

131. Asjaolu, et rikkumine võib toimuda ja seda ei pruugita niivõrd pika aja jooksul avastada ning et pikemas perspektiivis oleks võidud kasutada sotsiaalset manipulatsiooni suurema andmehulga muutmiseks, toob esile olulised probleemid vastutava töötleja IT-turbe süsteemis. Need tuleks viivitamata kõrvaldada, pöörates tähelepanu näiteks automatiseerimise läbivaatamisele ja muudatuste kontrollimisele, intsidentide avastamisele ja reageerimismeetmetele. Tundlikke andmeid, finantsteavet jms käsitsevatel vastutavatel töötlejatel on piisava andmeturbe tagamisel suurem vastutus.

Meetmed, mida tuleb tuvastatud riskide põhjal võtta		
Asutusesisene dokumenteerimine	Järelevalveasutuse teavitamine	Andmesubjektide teavitamine
✓	✓	✓