**ISIKUANDMETEGA SEOTUD RIKKUMISTELE**

**REAGEERIMISE PROTSEDUUR**

**1. SISSEJUHATUS**

See isikuandmetega seotud rikkumistele reageerimise protseduur („**protseduur**”) kirjeldab isikuandmetega (defineeritud allpool) seotud rikkumistest või rikkumiskahtlusest teatamise ja registreerimise protsessi.

Selle protseduuri eesmärk on tagada, et ettevõte tegeleks ja kõrvaldaks igasuguse isikuandmetega seotud rikkumise sündmuse kiiresti, et selle mõju oleks minimaalne ning et kõik seadusest tulenevad kohustused teavitada isikuandmetega seotud rikkumisest Andmekaitse Inspektsiooni („**AKI**“) ja/või rikkumisest mõjutatud isikut/isikuid kooskõlas isikuandmete kaitse üldmäärusega (määrus (EL) 2016/679) („**GDPR**”)) saaks õigeaegselt täita.

**2. MIS ON ISIKUANDMED?**

Isikuandmed on igasugused andmed, mis puudutavad ELis asuvat inimest ja mille alusel on võimalik seda inimest tuvastada („**isikuandmed**”). Isik on tuvastatav, kui tema isikut saab andmete põhjal ebaproportsionaalse pingutuseta mõistlikus ulatuses tuvastada. Tuvastamise aluseks võib olla näiteks nimi, isikukood, asukohateave, võrguidentifikaator või füüsiline, füsioloogiline, geneetiline, vaimne, majanduslik, kultuuriline või sotsiaalne tunnus või selliste tunnuste kombinatsioon.

**3. MIS ON ISIKUANDMETEGA SEOTUD RIKKUMINE?**

GDPRi definitsiooni kohaselt on isikuandmetega seotud rikkumine „*on turberikkumine, mille tagajärg on edastatavate, säilitatavate või muul viisil töödeldavate isikuandmete tahtmatu või ebaseaduslik hävimine, kaotsiminek, muutmine, lubamatu avaldamine või lubamatu juurdepääs neile andmetele*” („**isikuandmetega seotud rikkumine**”).

Isikuandmetega seotud rikkumine leiab aset siis, kui isikuandmeid loata või kogemata avaldatakse, need kaotsi lähevad või kui neid mis tahes muul viisil omavoliliselt, kogemata või ebaseaduslikult kogutakse, kasutatakse, registreeritakse, talletatakse või jagatakse. Isikuandmetega seotud rikkumise näited on: isikuandmeid sisaldava sülearvuti või mobiiltelefoni kaotsiminek või vargus; (kaitsmata) isikuandmeid sisaldava Exceli faili saatmine vastuvõtuks õigustamata isikule; palgaandmete printimine ja nende printerisse jätmine; isikuandmeid sisaldavasse süsteemi häkkimine ja/või failide kaotsiminek või vargus jne.

Igasugust andmeturbe rikkumisega seotud juhtumit nimetatakse „**andmekaitsejuhtumiks**”. Kui andmekaitsejuhtum ei hõlma isikuandmeid, pole tegemist isikuandmete rikkumisega. Lisaks pole mitte kõik isikuandmeid hõlmavad andmekaitsejuhtumid isikuandmetega seotud rikkumised. Näiteks ei pruugi isikuandmete kaotsiminek olla isikuandmetega seotud rikkumine, kui: i) isikuandmed on krüpteeritud või anonüümseks muudetud; ii) isikuandmetest on tehtud täielik ajakohane varukoopia ning iii) juurdepääsu isikuandmetele jälgitakse. Seetõttu tuleb juhtumipõhiselt otsustada, kas andmekaitsejuhtum kujutab endast isikuandmetega seotud rikkumist.

**4. MILLAL SEDA PROTSEDUURI KOHALDATAKSE?**

Kui andmekaitsejuhtum *ei hõlma* isikuandmeid, siis ei ole vaja seda protseduuri järgida. Kui andmekaitsejuhtum *hõlmab* isikuandmeid, võib olla tegemist isikuandmetega seotud rikkumisega ja seda protseduuri kohaldatakse. Kahtluste korral, kas on toimunud isikuandmetega seotud rikkumine, peaks ettevõte olukorda hindama ja vajadusel küsima nõu ka vastava valdkonna spetsialistidelt väljastpoolt ettevõtet.

**5. KUIDAS ISIKUANDMETEGA SEOTUD RIKKUMISEST TEATADA?**

On tähtis, et kõigist tegelikest või arvatavatest isikuandmetega seotud rikkumistest teatataks kohe järgmiste juhiste kohaselt.

**5.1 Esialgne teatamine**

Kui saate teada tegelikust või arvatavast isikuandmetega seotud rikkumisest, tuleb sellest teatada kohe ettevõtte tegevjuhile ja olemasolu korral andmekaitsespetsialistile või ettevõttes andmekaitse eest vastutavale isikule (edaspidi mõlema kohta „**andmekaitsespetsialist**“).

**5.2 Lahenduskava koostamine**

Kui on toimunud isikuandmetega seotud rikkumine, koostab ettevõtte tegevjuht koostöös andmekaitsespetsialistiga plaani isikuandmetega seotud rikkumise lahendamiseks. Selle protseduuri lisas 1 on voodiagramm isikuandmete rikkumise lahendamiseks.

Asjakohase lahenduskava koostamisel arvestab lahendusega tegelev meeskond järgmist:

* isikuandmetega seotud rikkumise teatises saadud andmeid;
* vajalikke toiminguid, mis on vaja isikuandmetega seotud rikkumise peatamiseks kohe teha;
* kas on vajalik teavitada AKI´t isikuandmetega seotud rikkumisest ja kui on, siis millest tuleb teatada;
* isikuandmetega seotud rikkumisest tulenevad võimalikud tagajärjed ettevõttele ja mõjutatud isikutele;
* meetmed, mida ettevõte sellel ajal rakendab ja/või saab rakendada, et mõjutatud isikute kahju vähendada;
* viis, kuidas rikkumisest mõjutatud isikuid isikuandmete rikkumisest teavitatakse, kas see on antud olukorras kohane; ja meetmed, mida inimesed saavad rakendada edasise kahju leevendamiseks;
* kas isikuandmetega seotud rikkumisega võib kaasneda ettevõtte vastutus või muude osapoolte (nt volitatud töötleja) vastutus;
* ettevõtte sisene (ja vajaduse korral väline) kommunikatsioon ja sellise kommunikatsiooni ajastus;
* kas lisaks AKI´le tuleks teavitada ka muid huvirühmi; ja
* mida saab isikuandmetega seotud rikkumisest õppida ja milliseid meetmeid rakendada, et püüda konkreetse rikkumise kordumist ja sarnaseid rikkumisi vältida.

**5.3 Kas AKI teavitamine on nõutav?**

Igast isikuandmetega seotud rikkumisest pole vaja AKI´t teavitada. Näiteks pole vaja AKI´t teavitada, kui isikuandmete rikkumisega ei kaasne tõenäoliselt ohtu ühelegi inimesele. Kui AKI´t siiski on vaja teavitada, teeb seda ettevõtte tegevjuht kui on teavitamise vajadust andmekaitsespetsialistiga arutanud.

Seega peab ettevõte hindama, millal on tegu ohuga füüsiliste isikute õigustele ja vabadustele. GDPRi põhjenduspunktid 75, 76 ja 85 selgitavad, et erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhtudel, kui:

* töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju;
* andmesubjektid võivad jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle;
* töödeldakse isikuandmete eriliike (delikaatseid isikuandmeid);
* tegeletakse profileerimisega;
* töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid;
* töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Andmesubjekti õigustele ja vabadustele tekkiva ohu tõenäosus ja tõsidus tuleks teha kindlaks lähtudes andmetöötluse laadist, ulatusest, kontekstist ja eesmärkidest. Ohtu tuleks hinnata objektiivse hindamise põhjal, millega tehakse kindlaks, kas andmetöötlustoimingutega kaasneb oht või suur oht.

Teade AKI´le tuleb edastada tarbetu viivituseta ja võimaluse korral hiljemalt 72 tundi pärast isikuandmetega seotud rikkumisest teadasaamist. Kui teadet ei edastata 72 tunni jooksul, tuleb esitada AKI´le selgitustega põhjendus viivituse kohta.

**5.4 Lahendamine**

Pärast AKI teavitamist ja AKI poolt tehtud tähelepanekute kaalumist peab ettevõtte tegevjuht andmekaitsespetsialistiga isikuandmetega seotud rikkumise käsitlemise ja lahendamise teemal nõu, lähtudes asjakohasest isikuandmetega seotud rikkumise lahenduskavast.

**6. MILLEST ON VAJA AKI´t TEAVITADA?**

Aruandes AKI´le tuleb teavitada järgmisest:

* isikuandmetega seotud rikkumise iseloom, muu hulgas puudutatud isikuandmete kategooriad ja inimeste kategooriad (nt töötajad või kliendid), mõjutatud inimeste arv ja ohustatud isikuandmete hulk;
* isikuandmetega seotud rikkumise eeldatavad tagajärjed;
* meetmed, mis on võetud või mida plaanitakse võtta tarvitusele isikuandmetega seotud rikkumise kõrvaldamiseks;
* meetmed, mida rikkumisest mõjutatud inimesed saavad tarvitusele võtta, et piirata isikuandmetega seotud rikkumisest tulenevaid kahjulikke tagajärgi; ja
* ettevõtte kontaktisiku nimi ja kontaktandmed lisateabe saamiseks isikuandmetega seotud rikkumise kohta.

NB! Rikkumisteadete edastamise hõlbustamiseks on AKI´l kavas oma võrgulehele luua vastav veebiteenus.

**7. ISIKUANDMETEGS SEOTUD RIKKUMISEST TEATAMINE MÕJUTATUD INIMESTELE**

Isikuandmetega seotud rikkumisest mõjutatud inimest tuleb teavitada ainult juhul, kui isikuandmete rikkumisega kaasneb tõenäoliselt suur oht selle inimese õigustele ja vabadustele. Isikuandmete rikkumisest teatamine mõjutatud isikutele peab toimuma vastava lahenduskava kohaselt.

Töötlemistoimingute liigid, mis kujutavad oma laadi, ulatuse, konteksti ja eesmärkide poolest tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele on näiteks:

* uue tehnoloogia kasutamine. *See ei pea ilmtingimata olema ajalises plaanis uus, vaid võib olla näiteks tark- või riistvara, mis on turul juba mõnda aega olnud kättesaadav, kuid mida andmetöötleja ei ole seni kasutanud, kuid plaanib kasutusele võtta*;
* andmetöötlustoimingud on uut tüüpi ja vastutav töötleja ei ole nende osas varem andmekaitsealast mõjuhinnangut teostanud. *Näiteks uute toodete või teenuste arendamine ning pakkumine*;
* ulatuslikud isikuandmete töötlemise toimingud, mille eesmärk on töödelda suurt hulka isikuandmeid piirkondlikul, riiklikul või rahvusvahelisel tasandil ja mis võivad mõjutada paljusid andmesubjekte;
* avalike alade ulatuslik jälgimine, eriti kui kasutatakse elektroonilisi optikaseadmeid (nt videokaamerad korrakaitse või valve eesmärgil).

Andmesubjekti teavitamise eesmärk on lisaks ettevõttele võimaldada ka andmesubjektil endal võtta vajalikke ettevaatusabinõusid ohu leevendamiseks. Teates tuleks kirjeldada isikuandmetega seotud rikkumise olemust, samuti tuleks anda asjaomasele füüsilisele isikule soovitusi võimaliku kahjuliku mõju leevendamiseks.

Rikkumisest mõjutatud isikutele saadetav teavitus peab sisaldama vähemalt järgmist:

* isikuandmetega seotud rikkumise iseloom ja ulatus;
* meetmed, mis on isikuandmetega seotud rikkumise negatiivsete tagajärgede piiramiseks tarvitusele võetud;
* nii isikuandmetega seotud rikkumise tegelike kui ka eeldatavate tagajärgede kirjeldus; ja
* meetmed, mida ettevõte on tarvitusele võtnud või kavatseb isikuandmetega seotud rikkumise tagajärgede leevendamiseks rakendada.

Inimeste teavitamine pole vajalik, kui:

* ettevõte on rakendanud sobivaid tehnilisi ja organisatsioonilisi meetmeid, mis muudavad isikuandmed loetamatuks kõigile, kellel puudub õigus neile juurde pääseda, näiteks krüpteerimise kaudu;
* ettevõte on võtnud tarvitusele edasisi meetmeid, mis tagavad selle, et suur oht inimestele tõenäoliselt ei realiseeru; või
* see nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse tarvitusele muud sarnased meetmed, et rikkumisest puudutatud isikuid võrdselt teavitada.

Juhul kui ettevõte ei pea vajalikuks andmesubjekte informeerida, annab GDPRi artikkel 34(4) AKI´le siiski õiguse ettevõttelt vastavat teavitamist nõuda.

**8. RIKKUMISTE REGISTER**

Ettevõte peab pidama isikuandmetega seotud rikkumiste registrit, milles dokumenteeritakse kõik isikuandmetega seotud rikkumised („**register**”).

Registri eesmärk on: i) õppida isikuandmete rikkumisest ja sellest, kuidas sellega toime tuldi; ii) suuta anda täpseid vastuseid rikkumisest mõjutatud isikutelt ja/või AKI´lt saadud küsimustele ning iii) luua võimalus, et vajadusel AKI´le tõendada isikuandmetega seotud rikkumise menetlemiseks GDPR´is ettenähtud nõuete täitmist.

Iga isikuandmetega seotud rikkumise kohta kantakse registrisse järgmised andmed:

* isikuandmete rikkumisest teadasaamise/teavitamise kuupäev ja kellaaeg;
* mõjutatud isiku(te) nimi ja kontaktandmed;
* faktid ja üksikasjad isikuandmetega seotud rikkumise iseloomu kohta;
* isikuandmetega seotud rikkumise mõjude kirjeldus;
* kellele isikuandmete rikkumisest on teatatud ja miks; ning
* järelmeetmed pärast isikuandmete rikkumise avastamist (nt meetmed, mis takistavad isikuandmete rikkumise kordumist jne).

LISA 1

**Isikuandmetega seotud rikkumise protseduuri voodiagramm**

**Isikuandmetega seotud rikkumine**

Juhtum on lahendatud. Rikkumiste register on ajakohastatud. Arutage saadud õppetunde ja vajalikke järelmeetmeid.

Kui see on vajalik, korraldab ettevõtte tegevjuht või andmekaitsespetsialist AKI teavitamise 72 tunni jooksul ja hoiab huvirühmad asjaga kursis

Täiendav reageerimine ei ole nõutav

Ettevõtte tegevjuht ja/või andmekaitsespetsialist kaaluvad, kas AKI teavitamine on vajalik

**Ei ole vajalik**

Vajadusel ajakohastage rikkumiste registrit. Arutage saadud õppetunde ja järelmeetmeid. Täiendav reageerimine ei ole nõutav.

**Kas AKI teavitamine on vajalik?**

Ettevõtte tegevjuht ja/või andmekaitsespetsialist koostavad lahenduskava

**Lahenduskava koostamine**

**Ei ole isikuandmetega seotud rikkumist**

**Isikuandmetega seotud rikkumine**

**Hindamine**

**Teatamine**

Ettevõtte tegevjuht ning andmekaitsespetsialist hindavad, kas esineb isikuandmetega seotud rikkumine

Teavitage ettevõtte tegevjuhti ja andmekaitsespetsialisti

**Otsus ja registreerimine**

**AKI teavitamine**