ISIKUANDMETEGA SEOTUD RIKKUMISE KORD

SA Viljandimaa Arenduskeskus

Versioon kinnitatud: 01.02.2022

ISIKUANDMETEGA SEOTUD RIKKUMISE KORD

1. Käesolev isikuandmetega seotud rikkumise kord kohaldub koos Viljandimaa Arenduskeskus SA (edaspidi **MAK**) teiste isikuandmete töötlemist reguleerivate dokumentidega (sh privaatsustingimused, isikuandmete töötlemise üldtingimused, töötajate isikuandmete töötlemise tingimused). Käesolevas korras kasutatakse mõisteid tähenduses nagu need on defineeritud **MAK**-i isikuandmete töötlemise üldtingimustes.
2. Käesolevas dokumendis kirjeldatakse, kuidas tuleb toimida isikuandmetega seotud rikkumise korral. Isikuandmetega seotud rikkumine tähendab turvanõuete rikkumist, mis põhjustab isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.
3. Isikuandmetega seotud rikkumine võib tekkida või olla juba tekkinud näiteks olukorras, kui:
   3.1. isikuandmete töötlemise juures viibib isik, kellel puudub selleks luba;
   3.2. saadakse või üritatakse saada loata juurdepääs isikuandmete töötlemisele (sh valdusele, kus isikuandmeid töödeldakse). Tähelepanu tuleb pöörata näiteks juhtumitele, mil dokumentide järjekord või paigutus ruumis on muutunud, mõni uks või sahtel on avatud, töötlemiseks kasutatavate seadmete asukoht või kuvatav teave on muutunud jne.
   3.3. tavaline lubatud juurdepääs isikuandmetele on takistatud. Tähelepanu tuleb pöörata näiteks juhtumitele, kui ruumi võtmed on kadunud või õige salasõnaga ei ole võimalik seadmetele või kontodele juurde pääseda.
   3.4. isikuandmete koosseis (konkreetsete andmete sisu või nende maht) või vorm on muutunud;
   3.5. seade kuvab teavitusena hoiatusi (sh pahavara, ebaharilik sisselogimine vms) või veateateid;
   3.6. loata kustutatakse andmeid või hävitatakse andmeid säilitavaid seadmeid.
4. Kui töötaja on teadlik isikuandmetega seotud rikkumisest või kahtlustab, et isikuandmetega seotud rikkumine võib tekkida või olla juba tekkinud, siis on töötaja kohustatud:
   4.1. teavitama rikkumisest viivitamatult andmekaitsespetsialisti ja juhatust, kuid mitte hiljem kui 24 tunni jooksul teadasaamisest või kahtluse tekkimisest, täites selleks ettenähtud vormi „Teavitus isikuandmetega seotud rikkumisest“ (vt lisa 1, selle dokumendi lõpus);
   4.2. lõpetama isikuandmete töötlemise ja asjakohasel juhul töötlemiseks kasutatud IT-süsteemi kasutamise ning ootama tööandja täiendavaid juhiseid (sh juhiseid töötlemise jätkamise lubamiseks);
   4.3. hoiduma ise rikkumise kõrvaldamisest või selle üritamisest. Kui töötajal on ettepanekuid rikkumise kõrvaldamiseks, siis tuleb need edastada vormil „Teavitus isikuandmetega seotud rikkumisest“;
   4.4. dokumenteerima (näiteks pildistama ja kirjeldama) sõnumid, asjaolud, hoiatused või muud viited, mis seonduvad rikkumise või selle tekkimise riskiga.
5. Juhatus kohustub rikkumisest teavitama IT-süsteemide administraatorit, kui rikkumine on seotud IT-süsteemidega. Vastavate süsteemide administraator kohustub minimeerima rikkumise tekkimise, jätkumise ja/või kordumise võimaluse, muu hulgas kohustub administraator:
   5.1. vajadusel piirama võrkude ja/või serverite tööd ja ühenduvust;
   5.2. tagama võimalikul maksimaalsel tasemel rikutud andmete turvalisuse;
   5.3. analüüsima rikkumise laadi, ulatust ja allikat;
   5.4. võimalusel kõrvaldama rikkumise tekkepõhjuse ja astuma samme uute rikkumiste välistamiseks.

6. Kui isikuandmetega seotud rikkumine võib kujutada endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele on MAK-l vastutava töötlejana kohustus teavitada rikkumisest põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast rikkumisest teada saamist Andmekaitse Inspektsiooni. Teavituse on kohustatud koostama ja esitama andmekaitsespetsialist. Andmekaitsespetsialist võib teavituseks kasutada selleks ettenähtud vormi „Teavitus isikuandmetega seotud rikkumisest“.
7. Kui isikuandmetega seotud rikkumine võib kujutada endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele, on MAK-l vastutava töötlejana kohustus teavitada rikkumisest andmesubjekti, välja arvatud kui:
   7.1. MAK on kehtestanud asjakohased tehnilised ja korralduslikud kaitsemeetmed ja neid kohaldati isikuandmetega seotud rikkumisest mõjutatud isikuandmetele, kasutades eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsu õiguseta isikutele loetamatuks (näiteks krüpteerimine);
   7.2. MAK on võtnud hilisemad meetmed, mis tagavad, et punktis 1.7 osutatud suure ohu teke andmesubjektide õigustele ja vabadustele ei ole enam tõenäoline, või
   7.3. teavitamine nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse muu sarnane meede, millega teavitatakse kõiki andmesubjekte võrdselt tulemuslikul viisil.
8. Andmesubjekti teavitamise vajaduse üle otsustab ja teavituse teeb andmekaitsespetsialist.
9. Andmesubjekti rikkumisest teavitades tuleb esitada:
   9.1. andmekaitsespetsialisti või mõne teise täiendavat teavet andva kontaktisiku nimi ja kontaktandmed;
   9.2. kirjeldada isikuandmetega seotud rikkumise võimalikke tagajärgi;
   9.3. kirjeldada MTÜ MAK-i poolt võetud või võtmiseks kavandatud meetmeid isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

LISA 1 - teavitus isikuandmetega seotud rikkumisest

Teavituse esitaja andmed:

Äriühingu nimi:

Nimi:

Ametikoht:

E-post:

Telefon:

Muud kontaktandmed:

1. Palun kirjeldage isikuandmetega seotud rikkumist ja selle ulatust.
Selgitus: isikuandmetega seotud rikkumise laad, võimalusel täpsustada asjaomaste andmesubjektide kategooriad (kliendid, töötajad vms) ja nende ligikaudne arv ning isikuandmete asjaomaste kirjete liigid (nimed, kontaktandmed, kliendikaardi andmed vms) ja nende ligikaudne arv.
3. Palun kirjeldada isikuandmetega seotud rikkumise võimalikke tagajärgi.

4. Palun kirjeldage kavandatud meetmeid isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.
5. Palun kirjeldage edaspidiste rikkumiste vältimiseks kavandatavaid parandusmeetmeid.
6. Kas rikkumisega seoses on võimalik, et isikuandmed on loetavad juurdepääsuõiguseta isikutele või on andmed loetamatud (näiteks krüpteerimisest tulenevalt)?

7. Millal ja kuidas saite rikkumisest teada. Kui teavitus esitatakse hiljem kui 24 tunni jooksul rikkumisest teadasaamisest, siis esitada selle kohta põhjendus.