Alates 25.05.2018.a. jõustus Euroopa parlamendi ja nõukogu määrus nr 2016/679 isikuandmete kaitse üldmäärus (edaspidi ÜM). ÜM Art 24 lg 1 paneb kõigile vastutavatele töötlejatele kohustuse rakendada asjakohaseid tehnilise ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete töötlemist kooskõlas ÜMga. ÜM Art 33 ja 34 sätestavad isikuandmete töötleja teavitus- ja dokumenteerimiskohustuse isikuandmetega seotud rikkumise korral. Arvestades ÜM sätestatud kohustusega rakendada korralduslikke meetmeid mh küsimustes, millised puudutavad isikuandmete töötleja käitumist isikuandmetega seotud rikkumiste korral, on vajalik korraldusliku meetmena Art 24 lg 1 täitmiseks kehtestada alljärgnev Isikuandmete rikkumisest teavitamise ja rikkumise dokumenteerimise kord.

***Ettevõtte nimi***

Isikuandmete rikkumisest teavitamise ja rikkumise dokumenteerimise kord

**I. Üldsätted**

1. ÜM Art 33 lg 5 sätestab Vastutava töötleja kohustuse dokumenteerida kõik isikuandmetega seotud rikkumised, sealhulgas isikuandmetega seotud rikkumise asjaolud, selle mõju ja võetud parandusmeetmed. Dokumendid võimaldavad Andmekaitse Inspektsioonil (AKI) kontrollida ÜM nõuete täitmist.

2. …………………. (edaspidi Ettevõte) töötajad teavitavad viivituseta ………………………….(ametikoht) …….…………….., tel ……………………, e-post …………………… isikuandmetega seotud rikkumisest või rikkumise ohust ning teevad seda võimalusel oma vahetu juhi kaudu. Vastav info võib andmekaitsespetsialistini jõuda ka muude allikate kaudu (andmesubjekt, uudiskanalid, e-kirjad kolmandatelt isikutelt jne). Selline esmane teavitus dokumenteeritakse ning selle tulemusel algab *isikuandmete rikkumise menetlus*, millise menetlejaks on andmekaitsespetsialist (AKS) ja juhatus või selle poolt selleks juhtumiks juhatuse poolt konkreetselt volitatud isik (edaspidi Menetleja).

**II. AKI teavitamine vastutava töötlejana**

3. Menetleja hindab menetluse käigus viivituseta, kas konkreetne isikuandmetega seotud rikkumine võib põhjustada füüsilistele isikutele füüsilise, materiaalse või mittemateriaalse kahju, nagu kontrolli kaotamine oma isikuandmete üle või õiguste piiramine, diskrimineerimine, identiteedivargus või pettus, rahaline kahju, pseudonümiseerimise loata tühistamine, maine kahjustamine, ametisaladusega kaitstud andmete konfidentsiaalsuse kadu või mõni muu tõsine majanduslik või sotsiaalne kahju asjaomasele füüsilisele isikule (edaspidi Oluline kahju). AKS’i hinnang dokumenteeritakse.

4. Olulise kahju tekkimise võimaluse või ohu korral teatab Menetleja põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist Andmekaitse Inspektsiooni (AKI) kodulehel <http://www.aki.ee/et/poordu-inspektsiooni-poole/rikkumisteate-edastamine> olevas ettenähtud vormis täidetuna ja edastatuna aadressile info@aki.ee.

5. Kui 72 tunni jooksul teatamine ei ole võimalik, lisab Menetleja selle hilinemise põhjused ning vastav teave antakse järk-järgult ilma põhjendamatu viivituseta. Kogu edastatud teave dokumenteeritakse.

6. Kas info edastada krüpteerituna või mitte, on AKI jätnud iga vastutava töötleja enda otsustada. Sellest tulenevalt edastab Menetleja andmed krüpteerimata või krüpteeritud kujul vastavalt oma äranägemisele.

7. AKI võib nõuda lisaks esialgsele teatisele ka põhjendamatu viivituseta lisateavet. Menetleja on valmis viivituseta vastavat teavet edastama. Kogu edastatud lisateave dokumenteeritakse.

8. Kui isikuandmete rikkumise hindamise tulemusel jõuab Menetleja tulemusele, et rikkumise näol ei ole tegemist Olulise kahjuga, peab hindamise aluseks olema suutlikkus kooskõlas vastutamise põhimõttega tõendada, et selle rikkumise tulemusena ei teki tõenäoliselt ohtu füüsilise isiku õigustele ja vabadustele. Vastavad tõendid dokumenteeritakse.

**III. Vastutava töötleja teavitamine Volitatud töötlejana.**

9. Olukorras, mil isikuandmete töötlemisel ollakse volitatud töötleja rollis, toimub p 1-8 kirjeldatud dokumenteeritud menetlus arvestades volitatud töötleja rolli erisusi. Selliselt teavitatakse vastutavat töötlejat (mitte AKIt) põhjendamatu viivituseta pärast isikuandmetega seotud rikkumisest teada saamist. Selles teates peab olema vähemalt alljärgnev teave:

9.1. isikuandmetega seotud rikkumise laadi kirjeldus ning võimaluse korral asjaomaste andmesubjektide kategooriad ja ligikaudne arv ning isikuandmete asjaomaste kirjete liigid ja ligikaudne arv;

9.2. andmekaitsespetsialisti või mõne teise täiendavat teavet andva kontaktisiku nimi ja kontaktandmed;

9.3. isikuandmetega seotud rikkumise võimalikke tagajärgede kirjeldus;

9.4. vastutava töötleja poolt võetud või võtmiseks kavandatud meetmete kirjeldus isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

**IV. Andmesubjekti teavitamine**

10. Kui isikuandmetega seotud rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele, teavitab Ettevõte vastutava töötlejana andmesubjekti põhjendamatu viivituseta isikuandmetega seotud rikkumisest.

11. vastavas teates märgitakse ära vähemalt järgmine info:

11.1. andmekaitsespetsialisti või mõne teise täiendavat teavet andva kontaktisiku nimi ja kontaktandmed;

11.2. isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldus;

11.3. vastutava töötleja poolt võetud või võtmiseks kavandatud meetmete kirjeldus isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

12. teavitus ja selle sisu dokumenteeritakse.

13. teavitamine ei ole vajalik kui:

13.1. Ettevõte on kehtestanud asjakohased tehnilised ja korralduslikud kaitsemeetmed ja neid kohaldati isikuandmetega seotud rikkumisest mõjutatud isikuandmetele, kasutades eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsuõiguseta isikutele loetamatuks (näiteks krüpteerimine);

13.2. Ettevõte on võtnud kasutusele hilisemad meetmed, mis tagavad, et suure ohu teke andmesubjektide õigustele ja vabadustele ei ole enam tõenäoline

13.3. See nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse muu sarnane meede, millega teavitatakse kõiki andmesubjekte võrdselt tulemuslikul viisil.

14. Vastav mitteteavitamise põhjus koos seda tõendavate tõenditega dokumenteeritakse.

**V. Isikuandmete rikkumise menetlus**

15. Kogu isikuandmete rikkumise menetluse käigus dokumenteeritu koondatakse ühte toimikusse. Toimik peab olema kronoloogiline ja süstematiseeritud.

16. Lisaks punktides 1-14 kirjeldatud dokumenteerimisele kuuluvatele dokumentidele, peab toimik sisaldama ka tõendeid isikuandmete rikkumisega seotud kahju lahendamise ja kahjuliku mõju leevendamiseks osas tarvitusele võetud meetmete toimimise kohta kuni nende reaalse mõju lõppemiseni.

17. Toimik peab sisaldama ka AKI poolt kõiki asjas tähtsust omavaid päringuid, dokumente, ettekirjutusi jms, mis võib kaasa tuua ettevõttele õigusi või kohustusi.

18. Kui ÜM kohased teavitused on tehtud, AKI poolt vastava rikkumise osas menetlus lõpetatud ning kahjude osas selge, et nõudeid ei ole, kuulub isikuandmete rikkumise menetluslõpetamisele.

19. Menetleja lõpetab isikuandmete rikkumise menetluse lõppaktiga, millises ta kirjeldab ära lühidalt kogu kaasuse, asjas tähtsust omavad faktilised asjaolud ning lõpplahenduse, kuidas rikkumine lahendati.

20. Toimikud digitaliseeritakse ja neid hoitakse elektroonilisel kujul Ettevõtte serveris. Paberkandjal olevatest dokumentidest säilitatakse ja arhiveeritakse paralleelselt vaid originaaldokumendid. Toimikuid ja originaaldokumente hoitakse 13 aastat rikkumisest, peale mida digitaliseeritud toimik kustutatakse ning originaaldokument hävitatakse.