Raamlepingu lisa 4

ANDMETÖÖTLUSE LEPING

Päästeamet (edaspidi vastutav töötleja), registrikood 70000585, aadress Raua 2, 10124 Tallinn, keda esindab põhimääruse alusel peadirektor Margo Klaos
ja
Meliva AS, registrikood 10303948, aadress Rävala pst 5, 10143 (edaspidi Volitatud töötleja), mida esindab seaduse ja volituse alusel volitatud esindaja Marek Goldman teiselt poolt,

mõlemad eraldi edaspidi nimetatud ka Pool ja koos Pooled, sõlmisid käesoleva andmetöötluse lepingu (edaspidi Leping) alljärgnevatel tingimustel:

1. LEPINGU ESE

1.1. Volitatud töötleja osutab Vastutavale töötlejale lepingu (edaspidi Põhileping) alusel esmase ja perioodilise tervisekontrollide teostamise ning töötleb selle raames Vastutava töötleja töötajate isikuandmeid volitatud töötlejana.

2. MÕISTED

2.1. Kolmas isik – iga füüsiline või juriidiline isik, kes ei ole Lepingu Pooleks ning kõik Poolte sellised töötajad ja/või teenuste osutajad, kes vahetult ja otseselt ei tegele täiendavate lepingutega kokkulepitud tööde teostamisega ja teenuste osutamisega.

2.2. Isikuandmete kaitse üldmäärus – Euroopa Parlamendi ja Nõukogu Määrus (EL) 2016/679, edaspidi ka IKÜM.

2.3. Kohaldatavad andmekaitse õigusaktid – on mis tahes kohaldatavad õigusaktid, mis on seotud andmete kaitsmise ja turvalisusega, sealhulgas eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv (Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris) ja isikuandmete kaitse üldmäärus (Euroopa Parlamendi ja nõukogu määrus 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta, edaspidi IKÜM) ja nende muudatused, asendused või pikendused (edaspidi koos: EL õigusaktid), kõik täitmiseks kohustuslikud riigisisesed seadused, millega rakendatakse ELi õigusakte, ja muud täitmiseks kohustuslikud andmekaitse või andmete turvalisuse direktiivid, seadused, määrused ja otsused, mis on vastaval ajal kehtivad.

2.4. Mõisted „isikuandmete töötlemine“, „isikuandmed“, „andmesubjekt“, „isikuandmetega seotud rikkumine“ on sellise tähendusega, mis neile on omistatud isikuandmete kaitse üldmääruses.

3. ISIKUANDMETE TÖÖTLEMISE NÕUDED NING POOLTE ÕIGUSED JA KOHUSTUSED

3.1. Vastutava töötleja õigused ja kohustused

3.1.1. Vastutav töötleja nõustub ja kinnitab, et isikuandmete töötlemine Lepingu täitmise raames Vastutava töötleja poolt on seaduslik vastavalt Kohaldatavatele andmekaitse õigusaktidele.

3.1.2. Vastutav töötleja esitab Volitatud töötlejale nõudmisel vajaliku teabe, mida Volitatud töötleja vajab Lepingust tulenevate kohustuste täitmiseks.

3.1.3. Vastutav töötleja tagab isikuandmete töötlemise vastavuse Kohaldatavates andmekaitse õigusaktides sätestatud nõuetega ning kehtestab isikuandmete kaitseks

organisatsioonilised, füüsilised ja tehnilised turvameetmed, eelkõige on eelnimetatud meetmed loetletud Lepingu lisas nr 1.

3.1.4. Vastutaval töötlejal on õigus regulaarselt (sh enne Põhilepingu sõlmimist või selle täitmisega alustamist) kontrollida Volitatud töötleja poolt isikuandmete töötlemise vastavust Kohaldatavate andmekaitse õigusaktidele, samuti Vastutava töötleja regulatsioonide nõuetele, sh kontrollida asjakohaste turvameetmete olemasolu. Auditite teostamisel arvestab Vastutav töötleja Volitatud töötleja äritegevusega ja viib auditid läbi Volitatud töötlejat ja tema igapäevast tegevust võimalikult vähekoormaval viisil.

3.1.5. Vastutaval töötlejal on õigus nõuda Volitatud töötlejalt kirjalikku enesehindamise vormi täitmist ja esitamist, et tuvastada Kohaldatavate andmekaitse õigusaktide nõuete täitmist mis tahes ajal enne Lepingu sõlmimist ja Lepingu kehtivuse ajal.

3.2. Volitatud töötleja õigused ja kohustused

3.2.1. Volitatud töötleja tagab, et tema ja tema volitatud isikud ei töötle isikuandmeid suuremas ulatuses ega muudel eesmärkidel, kui on vajalik Volitatud töötleja poolt Vastutava töötlejaga sõlmitud Põhilepingu, käesoleva andmetöötluslepingu ja IKÜMi nõuete täitmiseks.

3.2.2. Volitatud töötleja kohustub vastama Kohaldatavates andmekaitse õigusaktides, samuti Vastutava töötleja regulatsioonides, juhistes ja korraldustes Volitatud töötlejale kehtestatud nõuetele.

3.2.3 Volitatud töötleja kohustub tagama andmesubjektide õiguste nõuetekohase kaitse vastavalt Kohaldatavatele andmekaitse õigusaktidele, Lepingule ning Vastutava töötleja antud korraldustele, juhistele ja asjakohastele regulatsioonidele.

3.2.4. Volitatud töötleja kohustub täitma kõiki Vastutava töötleja poolt teenuse osutamise seoses antud korraldusi. Volitatud töötleja kohustub teavitama viivitamatult Vastutavat töötlejat, kui Volitatud töötleja hinnangul toob Vastutava töötleja antud korraldus või juhis kaasa Kohaldatavate andmekaitse õigusaktide rikkumise.

3.2.5. Volitatud töötleja kohustub tutvuma Vastutava töötleja poolt kehtestatud isikuandmete kaitse organisatsiooniliste, füüsiliste ja tehniliste turvameetmetega ning neid järgima.

3.2.6. Volitatud töötleja kohustub ka iseseisvalt rakendama isikuandmete kaitseks organisatsioonilisi, füüsilisi ja tehnilisi turvameetmeid, mis vastavad Kohaldatavate andmekaitse õigusaktide nõuetele. Turvameetmete rakendamisel võtab Volitatud töötleja arvesse töötlemise laadi, eesmärki, konteksti ja ulatust.

3.2.7. Vastutava töötleja nõudmisel kohustub Volitatud töötleja tutvustama isikuandmete kaitseks tarvitusele võetud turvameetmeid ja nende muudatusi Vastutavale töötlejale.

3.2.8. Volitatud töötleja kohustub teostama regulaarselt isikuandmete töötlemist puudutavas osas turvakontrolle ning Vastutava töötleja nõudmisel esitama 10 päeva jooksul nõudmise esitamisest vastavate kontrollide tulemused ja kokkuvõtted, milles sisalduvad vähemalt ülevaadet riskidest, riskide maandamiseks ja kõrvaldamiseks kasutusele võetud meetmeid ning rakendatud uuendusi.

3.2.9. Volitatud töötleja kohustub esitama Vastutavalt töötlejalt tasu nõudmata kõik andmed ja dokumentatsiooni ning osutama abi, mis on Vastutavale töötlejale vajalik, et täita Kohaldatavate andmekaitse õigusaktide kõiki nõudeid ja tõendada nimetatud nõuetele vastavust Lepinguga seotud isikuandmete osas, samuti võimaldama auditite tegemist regulaator- ja/või järelevalveasutuste poolt või Vastutava töötleja või tema esindaja poolt ja aitama nendele kaasa. Kui auditi käigus tuvastatakse Volitatud töötleja poolne käesoleva andmetöötluskokkuleppe või

turvanõuete rikkumine, sh kui rikkumise on põhjustanud tema sidusettevõtjad, nõustajad, alltöövõtjad või muud esindajad, kannab Volitatud töötleja Vastutava töötleja auditi kulud.

3.2.10. Volitatud töötleja kohustub säilitama ja hoidma kättesaadavana ajakohaseid andmeid töötlemistoimingute kohta (töötlustoimingute register IKÜM mõistes), sealhulgas andmete töötlejana tegutseva iga isiku nime, kontaktandmete kohta, Vastutava töötleja nimel tehtud töötlemise liikide kohta, ning esitama Vastutava töötleja taotlusel ja põhjendamata viivituseta Vastutavale töötlejale käesolevas punktis sätestatud dokumentatsiooni, et Vastutav töötleja saaks järgida Kohaldatavaid andmekaitse õigusakte.

3.2.11. Volitatud töötleja kohustub vastama Vastutava töötleja päringutele ning esitama kogu päringus palutud asjakohase informatsiooni seoses Lepingu nõuetele vastavusega 10 päeva jooksul alates vastava päringu kättesaamisest.

3.2.12. Volitatud töötleja kohustub hoidma Vastutava töötleja kaudu teatavaks saanud töödeldavad isikuandmed eraldi kolmandate isikute ja enda andmetest.

3.2.13. Volitatud töötleja kohustub hoidma isikuandmeid konfidentsiaalselt (st tagama, et andmetele ei saaks juurdepääsu selleks õigustamata isikud, sh Volitatud töötleja töötajad, kes ei osale Põhilepingu või käesoleva andmetöötluskokkuleppe täitmisel) ja tagama, et kõiki isikuid, keda on volitatud isikuandmeid töötlema, on teavitatud nende konfidentsiaalsest iseloomust, nad on saanud asjakohase koolituse oma kohustuste kohta ja nad on võtnud endale konfidentsiaalsuskohustuse või neile kehtib asjakohane seadusest tulenev konfidentsiaalsuskohustus.

3.2.14. Volitatud töötleja kohustub teavitama viivitamatult, kuid mitte hiljem kui 24 h jooksul Vastutavat töötlejat Lepingu ning Kohaldatavate andmekaitse õigusaktide nõuete rikkumisest, samuti mistahes Volitatud töötlejale esitatud kaebustest seoses tema poolt isikuandmete kaitse nõuete rikkumisega ning vastavate olukordade tekkimisel lahendama need ka võimalikult kiiresti, vältimaks edasist kahju ja leevendamaks juhtumi mõjusid. Isikuandmetega seotud rikkumiste korral võtab Volitatud töötleja koheselt kasutusele asjakohased meetmed rikkumise lahendamiseks, kahjulike mõjude leevendamiseks ja ennetamiseks tulevikus.

3.2.15. Volitatud töötleja kohustub edastama punkti 3.2.14 kohase teavituse andmekaitse@paasteamet.ee lisades isikuandmetega seotud rikkumise teavitusele juurde:
- rikkumise aeg;
- rikkumise asjaolud;
- miks rikkumine juhtus;
- rikkumisest puudutatud isikuandmeid sisaldavate kirjete arv;
- millised isikuandmeid rikkumine puudutab;
- rikkumisest puudutatud isikute arv;
- milliseid isikute kategooriaid rikkumine puudutab;
- võimalikud tagajärjed rikkumisest puudutatud isikutele;
- kasutusele võetud meetmed rikkumise lahendamiseks, kahjulike mõjude leevendamiseks ja ennetamiseks tulevikus;
- rikkumise piiriülene mõju.

3.2.16. Olukorras, kus Volitatud töötlejal esineb selline isikuandmetega seotud rikkumine, mis puudutab mitmete erinevate vastutavate töötlejate töödeldavaid isikuandmeid ning IKÜM artikli 33 kohaselt tuleb sellisest rikkumisest teavitada Eesti Andmekaitse Inspektsiooni, volitab Vastutav töötleja Volitatud töötlejat esitama rikkumisteate inspektsioonile ka Vastutava töötleja nimel. Rikkumisteates tuleb muuhulgas välja tuua, et rikkumisteade esitatakse ka Päästeameti nimel. Volitatud

töötleja kohustub sellise rikkumisteate esitamisest eelnevalt teavitama Vastutavat töötlejat.

3.2.17. Volitatud töötleja kohustub teavitama viivitamatult Vastutavat töötlejat, kui Volitatud töötleja suhtes algatatakse menetlus, mis võib tuua kaasa hüvitamise nõude või trahvi Kohaldatavate andmekaitse õigusaktide alusel. Sellise menetluse alustamise korral Volitatud töötleja:
- esitab Vastutavale töötlejale üksikasjad (sealhulgas konkreetsed rikkumisega seotud süüdistused);
- esitab Vastutavale töötlejale teabe ja osutab abi, mida Vastutav töötleja taotleb;
- ei takista Vastutava töötleja aktiivset osavõttu menetlusest (kasutades õigusabi omal kulul).

3.2.18. Kui andmesubjekt, järelevalve- või valitsusasutus (nt Andmekaitse Inspektsioon) või muu kolmas isik soovib Volitatud töötlejalt Vastutava töötlejaga sõlmitud lepingulise suhte alusel töödeldavaid isikuandmeid, suunab Volitatud töötleja vastava soovi Vastutavale töötleja kontaktile andmekaitse@paasteamet.ee . Volitatud töötlejal ei ole lubatud avaldada isikuandmeid ega muud teavet isikuandmete töötlemise kohta ilma Vastutava töötleja eelneva kirjaliku nõusolekuta, välja arvatud juhul, kui Volitatud töötleja on kohustatud avaldama vastavaid andmeid kohustuslike Euroopa Liidu või liikmesriigi õigusaktide alusel. Viimasel juhul teavitab Volitatud töötleja viivitamata Vastutavat töötlejat taotlusest seadusega lubatud ulatuses, kuid igal juhul enne taotlusele vastamist.

3.2.19. Volitatud töötleja kohustub mitte sõlmima alltöövõtulepinguid isikuandmete töötlemiseks, mitte edastama isikuandmeid Kolmandatele isikutele ega andma neile andmetele ligipääsu või kaasama neid isikuandmete töötlemisse ilma Vastutava töötleja eelneva kirjaliku nõusolekuta. Vastava nõusoleku andmise korral on Volitatud töötleja poolt isikuandmete edastamise tingimuseks, et vastavale kolmandale isikule kehtestatakse enne isikuandmete edastamist samad andmekaitse kohustused, nagu on sätestatud Lepingus, ning Volitatud töötleja vastutab ka kolmanda isiku vastavate kohustuste täitmise eest ja rikkumiste korral. Volitatud töötleja poolt kasutatavad alltöötlejad, kelle osas on Vastutav töötleja nõusoleku andnud.

3.2.20. Volitatud töötleja töötleb isikuandmeid vaid Euroopa Liidus või Euroopa Majanduspiirkonnas ning ei edasta andmeid Euroopa Liidust või Euroopa Majanduspiirkonnast väljapoole ega võimalda andmetele ligipääsu nendele isikutele, kes asuvad väljaspool eelnimetatud piirkonda. Tarkvara, selle komponendid ning liidesed (sh masskirja saatmise tarkvara), mida Volitatud töötleja kasutab Vastutava töötleja nimel isikuandmete töötlemiseks, peab isikuandmeid töötlema Euroopa Liidus, Euroopa Majanduspiirkonna lepinguriigis või Euroopa Komisjoni adekvaatsusotsusega riigis/ettevõttes. IKÜM V peatüki mõttes kolmandas, ebapiisava andmekaitse tasemega riigis oleva allvolitatud töötleja kasutamise korral peab Volitatud töötleja tagama ja tõendama, et allvolitatud töötleja puhul on täidetud IKÜM V peatüki nõuded (eeskätt sõlmitud Euroopa Komisjoni standardsed andmetöötlustingimused, teostatud piiriülese andmeedastuse mõjuhinnang ning rakendatud täiendavad kaitsemeetmed).

3.2.21. Volitatud töötleja kohustub tagastama kokkulepitud vormis ja/või hävitama (Vastutava töötleja valikul) kõik Vastutava töötleja nimel töödeldavad isikuandmed Põhilepingu lõppedes või lõpetades. Volitatud töötleja esitab Vastutava töötleja nõudmisel vastava tõestuse.

4. VASTUTUS

4.1. Lepingus ettenähtud kohustuste mitte täitmisel või mittenõuetekohasel täitmisel vastutab Pool õigusaktides ja poolte vahel sõlmitud punktis 1.1. viidatud Põhilepingus ettenähtud korras.

4.2. Lepingu rikkumise tagajärjel kahju saanud Poolel on õigus esitada kahju tekitanud Poolele nõue tekitatud kahju hüvitamiseks.

4.3. Lepingut rikkunud Pool kohustub tasuma kahjunõude teisele Poolele 30 (kolmekümne) kalendripäeva jooksul alates sellekohase nõude laekumise päevast.

5. LEPINGU KEHTIVUS

5.1 Leping jõustub alates allakirjutamise hetkest ja kehtib kuni Volitatud töötlejaga sõlmitud Põhilepingu lõppemiseni või lõpetamiseni. Põhilepingu lõpetamine ei lõpeta Volitatud töötleja kohustust järgida isikuandmete konfidentsiaalsuse nõuet.

5.2 Lepingu muutmine on võimalik vaid Poolte kirjalikul kokkuleppel. Päästeameti kontaktaadress on andmekaitse@paasteamet.ee.

5.3 Lepingule kohaldub Eesti õigus ning Lepingust tulenevad vaidlused lahendatakse Harju Maakohtus.

Poolte allkirjad:

(allkirjastatud digitaalselt) (allkirjastatud digitaalselt)

LEPINGU LISA 1 – TURVANÕUDED

1. Mõisted

1.1. Vastutava töötleja andmed on isikuandmed käesoleva lepingu sõnastuses, konfidentsiaalne
informatsioon teenuse osutamise lepingu sõnastuses ja muud andmed, mis Volitatud töötlejale teenuse osutamise käigus teenusega seoses teatavaks saavad.

1.2. Infotöötlusvahendid on infosüsteem, -teenused või -taristu või füüsilised asukohad, kus need asuvad.

1.3. Logimine on info või sündmuste üksikasjade registreerimine organiseeritud registreerimissüsteemi, tavaliselt järjestatuna info või sündmuste toimumise järjekorras.

1.4. Turvaintsident on soovimatu või ootamatu infoturvasündmust, mis võib kahjustada organisatsiooni tegevust ja/või ähvardada teabe turvalisust.

1.5. Turvameede on riski muutev abinõu, organisatsiooniline korraldus või protsess, mis aitab säilitada IT-süsteemide turvakvaliteediga seotud omadusi.

1.6. Turvaintsident on infosüsteemi kasutamise teel tekitatud sündmus, mille tagajärjeks on tegelik või võimalik kahjulik toime infosüsteemile ja/või selles olevale teabele.

2. Rakendusala

2.1 Turvameetmeid tuleb rakendada, kui Volitatud töötleja töötleb Vastutava töötleja andmeid.

3. Volitatud töötleja üldine vastutus

3.1. Volitatud töötleja vastutab täielikult selle eest, et Volitatud töötleja personal järgib kehtestatud turvanõudeid.

3.2. Volitatud töötleja rakendab turvanõuete järgimise tagamiseks nõutavad turvameetmed enne
Vastutava töötleja jaoks mis tahes ülesande täitmise alustamist.

3.3. Volitatud töötleja tagab, et Vastutava töötleja andmete töötlemine toimub kooskõlas turvameetmetega.

3.4. Volitatud töötleja ei võimalda Lepingut rikkudes ühelegi isikule juurdepääsu (see võib puudutada ka uut, laiendatud, uuendatud, pikendatud või muul viisil muudetud reaalajalist juurdepääsu üle võrgu) Vastutava töötleja andmetele ilma Vastutava töötleja eelneva kirjaliku nõusolekuta.

4. Turvanõuded

4.1. Volitatud töötleja kaitseb infotöötlusvahendeid välis- ja keskkonnaohtude ja -riskide eest, sealhulgas voolu-/kaablirikete ja toetavate teenuste riketest põhjustatud muude katkestuste eest. See hõlmab füüsilist perimeetri ja juurdepääsu kaitsmist

4.2. Volitatud töötleja tuvastab ja hindab konfidentsiaalsuse, tervikluse ja käideldavusega seotud turvariske ning rakendab vastava hindamise alusel asjakohaseid tehnilisi ja organisatoorseid meetmeid tagamaks riskile vastava turvataseme.

4.3. Volitatud töötlejal on dokumenteeritud protsessid ja praktikad oma tegevuses esinevate riskidega tegelemiseks.

4.4. Volitatud töötleja hindab perioodiliselt infosüsteemide ning info töötlemise, talletamise ja edastamisega seotud riske.

4.5. Volitatud töötleja tagab võime taastada õigeaegselt Vastutava töötleja andmete käideldavus ja neile juurdepääs füüsilise või tehnilise intsidendi korral.

4.6. Volitatud töötleja rakendab kahjurvara kaitset tagamaks, et Volitatud töötleja poolt Vastutava töötleja teenuste tarnimisel kasutatav tarkvara on kahjurvara eest kaitstud.

4.7. Volitatud töötleja rakendab infosüsteemide kaitsmiseks võrkude turvameetmed, nt teenusetasemed, tulemüüri ja lahususe.
4.8. Volitatud töötleja teeb kriitilise tähtsusega infost varukoopiaid ja testib varukoopiaid tagamaks, et infot on võimalik vastavalt Vastutava töötlejaga kokku lepitule taastada.
4.9. Volitatud töötleja logib ja jälgib tegevusi, nt töödeldavate andmete loomist, lugemist, kopeerimist, muutmist ja kustutamist, aga ka erandeid, rikkeid ja infoturbe sündmusi ning vaatab neid regulaarselt üle. Lisaks kaitseb ja talletab Volitatud töötleja (vähemalt üheks aastaks) logi infot ning esitab nõudmise korral jälgimisandmed Vastutavale töötlejale turvaintsidentide korral. Logikirjest peab olema võimalik tuvastada tegevuse teostaja, tegevuse teostamise aeg, tegevuse sisu, tegevuse allikas (millisest seadmest tegevus teostati) ning tegevuse tulemus (näiteks: õnnestus, ebaõnnestus, tehniline viga vms).
4.10. Volitatud töötleja haldab kõigi asjakohaste tehnoloogiate, nt operatsioonisüsteemide, andmebaaside ja rakenduste turvanõrkusi proaktiivselt ja õigeaegselt.
4.11. Volitatud töötleja ei kasuta uuendamata kolmanda osapoole tarkvara. Kõik kolmanda osapoole pakutava tarkvara uuendused tuleb installeerida ilma põhjendamatu viivituseta. Tarkvarauuenduste rakendamata jätmine on selge IKÜM nõuete rikkumine, mis on karistatav.
4.12. Volitatud töötleja tagab arenduse lahususe testimis- ja tootmiskeskkonnast.
4.13. Volitatud töötlejal on dokumenteeritud protsess tehniliste ja organisatoorsete meetmete tõhususe regulaarseks testimiseks ja hindamiseks, et tagada töötlemise turvalisust.
4.14. Volitatid töötlejal on dokumenteeritud protsessid ja praktikad riskide haldamiseks Vastutava töötleja nimel isikuandmete töötlemisel.
4.15. Volitatud töötlejal on kehtestatud infoturbepoliitika ja protseduurid, mille peab kinnitama Volitatud töötleja juhtkond. Need avaldatakse Volitatud töötleja organisatsioonis ja nendest teavitatakse vastavat Volitatud töötleja personali.
4.16. Volitatud töötleja vaatab perioodiliselt üle oma turvapoliitikad ja -protseduurid ning ajakohastab neid vajadusel.
4.17. Volitatud töötlejal on oma organisatsioonis määratud ja dokumenteeritud turvarollid ja -vastutused.
4.18. Volitatud töötleja nimetab vähemalt ühe isiku, kellel on asjakohane turbepädevus ja kes kannab vastutust turvameetmete rakendamise eest ning kes on Vastutava töötleja turbepersonalile kontaktisikuks.
4.19. Volitatud töötleja tagab, et Volitatud töötleja personal, kes töötlevad Vastutava töötleja poolt edastatud isikuandmeid, on teadlikud Lepinguga seotud info, vahendite ja süsteemide heakskiidetud kasutusest (sealhulgas kasutuspiirangutest vastavalt olukorrale).
4.20. Volitatud töötleja tagab, et turbeteemade eest vastutav Volitatud töötleja personal on koolitatud turvalisusega seotud ülesannete täitmiseks.
4.21. Volitatud töötleja tagab oma personalile perioodilise turvateadlikkuse koolituse.
4.22. Volitatud töötleja on sätestanud ja dokumenteerinud juurdepääsu reguleerimise poliitika juurdepääsuks vahenditele, asukohtadele, võrgule, süsteemile, rakendustele ja infole/andmetele (sealhulgas füüsilise, loogilise ja kaugjuurdepääsu nõuded), kasutajale juurdepääsu ja kasutussõiguste andmise protsess, protseduurid juurdepääsuõiguste tühistamiseks ning Volitatud töötleja personali juurdepääsuõiguste lubatud kasutusviisid.
4.23. Volitatud töötleja on rakendanud formaalse ja dokumenteeritud kasutajate registreerimise ja deregistreerimise protsessi juurdepääsuõiguste andmiseks.
4.24. Volitatud töötleja tagab, et Volitatud töötleja personalil on isiklik ja ainulaadne tunnus (kasutajatunnus) ja kasutatakse asjakohast autentimismeetodit, mis kinnitab ja tagab kasutajate tuvastamise.

4.25. Volitatud töötleja kajastab käesolevate Turvanõuete sisu oma Volitatud töötlejatega sõlmitud lepingutes, kes täidavad Lepingu alusel antud ülesandeid.
4.26. Volitatud töötleja teostab regulaarselt Volitatud töötleja poolt Turvanõuete järgimise seiret, ülevaatamist ja auditit.
4.27. Volitatud töötleja esitab Vastutava töötleja nõudmisel Vastutavale töötlejale tõenduse Volitatud töötleja poolt turvameetmete rakendatuse kohta (seda tõendab välise audiitori poolt väljastatud E-ITS auditi järeldusotsus või akrediteeritud sertifitseerimisasutuse poolt väljastatud ISO/IEC 27001 sertifikaat).

ISIKUANDMETEGA SEOTUD RIKKUMISTEST TEAVITAMISE JUHEND VOLITATUD TÖÖTLEJATELE

Juhendi eesmärk on reguleerida infovahetust Vastutava ja Volitatud töötleja vahel seoses isikuandmetega seotud rikkumiste avastamise, menetlemise ja teavitamisega.

1. Isikuandmetega seotud rikkumised

1.1. Rikkumine on turvaintsident, mis toob kaasa edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu. Rikkumisi on kolme liiki:

1.2.1 konfidentsiaalsuse rikkumine isikuandmete loata või juhuslik avalikustamine või andmetele ligipääs Näiteks, kui eraklientide kodused aadressid ja e-posti aadressid saavad kas tehnilise vea või inimliku eksituse tõttu avalikkusele veebis nähtavaks

1.2.2 terviklikkuse rikkumine isikuandmete loata või juhuslik muutmine

1.2.3 kättesaadavuse rikkumine isikuandmetele ligipääsu ajutine mitte võimaldamine või kui isikuandmed on alaliselt kadunud või hävitatud. Näiteks, kui andmed on kogemata kustutatud ja neid ei ole võimalik taastada või kui turvaliselt krüpteeritud andmete võti on kadunud vms. Rikkumine võib olla samaaegselt seotud loetletud liikide erinevate kombinatsioonidega. Volitatud töötleja on kohustatud tagama, et tema töötajad on rikkumiste ning rikkumisi puudutavate kohustuste osas koolitatud ja teavitatud. Vastavalt IKÜM-ile on Vastutaval töötlejal kohustus teatud rikkumistest teavitada viivitamatult (teatud juhul 72 tunni jooksul) järelevalveasutust ja/või andmesubjekti. Juhul, kui rikkumine toimub Volitatud töötleja valduses olevate isikuandmetega, tuleb Volitatud töötlejal teavitada Vastutavat töötlejat vastavalt andmetöötluslepingule.

2. Rikkumisest teavitamine

2.1 Andmetöötluslepingus sisalduva kokkuleppe kohaselt on Volitatud töötleja rikkumise või võimaliku rikkumise avastamisel või rikkumise kohta teavituse saamisel kohustatud:

- koheselt, enne rikkumisest teavitamist, kasutama oma pädevusele vastavaid asjakohaseid meetmeid, et rikkumisega kaasnevat võimalikku kahju vähendada. Näiteks teavitama ekslikult isikuandmeid sisaldava meili saanud isikut, et see meil koos selles sisalduvate isikuandmetega tuleb kustutada ja meilis sisalduvate isikuandmete töötlemine on ebaseaduslik.
- koheselt, aga mitte hiljem kui 24 tunni jooksul, teavitama rikkumisest Päästeameti kontaktmeilil andmekaitse@paasteamet.ee.
  Kui Volitatud töötleja ei ole kindel, kas rikkumine on toimunud, kuid tal on põhjendatud kahtlus rikkumise toimumise osas, tuleb siiski teavitus Päästeametile edastada, et Vastutav töötleja saaks juhtumit analüüsida ja vajadusel Volitatud

töötlejale juhiseid jagada. Rikkumise registreerimisel tuleb Volitatud Töötlejal edastada alljärgnev teave:

- rikkumise avastamise kuupäev ja kellaaeg,
- rikkumise toimumise aeg,
- rikkumise asjaolud,
- kuidas Volitatud töötleja sai rikkumisest teada,
- rikkumise tagajärg,
- mõjutatud isikuandmete liigid (näiteks isiku nimi, isikukood, aadress),
- mitu andmesubjekti on rikkumisest mõjutatud,
- milliseid isikute kategooriaid rikkumine puudutas,
- milline on rikkumise võimalik tagajärg andmesubjektile,
- kasutusele võetud meetmed rikkumise lahendamiseks, kahjulike mõjude leevendamiseks ja ennetamiseks tulevikus;
- rikkumise piiriülene mõju.

2.2 Juhul, kui Volitatud töötleja saab järelevalveasutustelt, andmesubjektilt või kolmandalt isikult päringu rikkumise kohta, on Volitatud töötleja kohustatud päringust koheselt teavitama kontaktmeilil andmekaitse@paasteamet.ee ja saama päringuga tegelemiseks täiendavad juhised. Täiendavate küsimuste korral on võimalik pöörduda kontaktmeilil andmekaitse@paasteamet.ee.

3. Rikkumiste tagajärjed

3.1 Rikkumine, kui seda asjakohaselt ja õigeaegselt ei käsitleta, võib põhjustada andmesubjektile füüsilist, materiaalset ja/või mittemateriaalset kahju, nagu näiteks:

- kontrolli kaotamine oma isikuandmete üle või õiguste piiramine,
- diskrimineerimine,
- identiteedivargus või pettus,
- rahaline kahju,
- maine kahjustamine,
- ametisaladusega kaitstud andmete konfidentsiaalsuse kadu jne.

3.2 Rikkumiste asjakohane ja õigeaegne käsitlemata jätmine võib kaasa tuua järelevalveasutuse menetluse koos õiguslike tagajärgedega (nt ettekirjutus, hoiatus, trahv jne), maine kahju, kahjunõuded.