KAITSERESSURSSIDE AMETI ISIKUANDMETE TÖÖTLEMISE JUHIS

1. ÜLDSÄTTED

1.1. Kaitseressursside Ameti (edaspidi amet) isikuandmete töötlemise juhis (edaspidi juhis) sätestab isikuandmete töötlemise põhimõtted, andmesubjekti õigused ja ameti kohustused isikuandmete töötlemisel ning turvameetmed isikuandmete kaitseks.

1.2. Käesolev juhis on täitmiseks kohustuslik kõikidele ameti isikuandmeid töötlevatele isikutele.

1.3. Amet lähtub isikuandmete töötlemisel **„Isikuandmete kaitse seadusest“**, **Euroopa Parlamendi ja nõukogu 25.05.2018 määrusest 2016/679** (isikuandmete kaitse üldmäärus – IKÜM, **„Avaliku teabe seadusest“**, ning **Andmekaitse Inspektsiooni juhistest**.

2. ISIKUANDMETE TÖÖTLEMISE PÕHIMÕTTED

2.1. Amet on vastutav töötleja ameti teenistujate ja lepingulises suhtes olevate isikute ning teatud juhtudel ka kolmandate isikute isikuandmete osas. Amet lähtub isikuandmete töötlemisel järgmistest põhimõtetest.

2.1.1. Seaduslikkuse põhimõte – amet kogub isikuandmeid vaid ausal ja seaduslikul teel. Amet töötleb isikuandmeid seadusega pandud ülesannete ja lepingutest tulenevate kohustuste täitmiseks ning oma õiguste realiseerimiseks.

2.1.1.1. Isikuandmeid töödeldakse reeglina isiku nõusolekul, millega isik kirjalikku taasesitamist võimaldavas vormis või selget tahet väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.

2.1.1.2. Isikuandmeid tohib töödelda sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate tegevuste käigus vastavalt isiku taotlusele.

2.1.1.3. Isikuandmeid tohib töödelda, kui see on vajalik andmetöötleja seadusest tulenevate kohustuse täitmiseks.

2.1.1.4. Isikuandmeid tohib töödelda avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks.

2.1.1.5. Isikuandmeid tohib töödelda hädaolukorras, kui see on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks.

2.1.1.6. Isikuandmeid tohib töödelda, kui see on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral. Õigustatud huvi olemasolul tuleb alati kaaluda igal üksikul juhul, kas andmesubjekt võib andmete kogumise ajal ja kontekstis mõistlikkuse piires eeldada, et isikuandmeid võidakse sellel otstarbel töödelda. Õigustatud huviks võib lugeda pettuste ennetamist, infoturbe tagamist, andmelekete kindlaks tegemist. Õigustatud huvi alusel töötlemisest tuleb isikut teavitada.

2.1.2. Eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas.

2.1.3. Minimaalsuse põhimõte – isikuandmeid võib koguda ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.

2.1.4. Kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal.

2.1.5. Andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks.

2.1.6. Turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.

2.1.7. Individuaalse osaluse põhimõte – andmesubjekti tuleb vajadusel teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja andmesubjektil on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

2.1.8. Läbipaistvuse põhimõte – isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud.

3. ANDMESUBJEKTID

3.1. Amet töötleb järgmiste andmesubjektide isikuandmeid:

3.1.1. ameti teenistujad

3.1.2. kaitseväekohustuslased

3.1.3. kaitseväekohustust võtta soovivad isikud;

3.1.4. ameti lepingupartnerid ja praktikandid;

3.1.5. ameti, valitsemisala tööle ja teenistusse kandideerivad isikud;

3.1.6. ameti külastajad;

3.1.7. ameti teenistujate alaealised lapsed ning kontaktisikud;

3.1.8. ameti arstlike komisjonide liikmed;

3.1.9. ameti poole pöördunud isikud;

3.1.10. ameti kodulehe külastajad;

3.1.11. ameti valvekaamerate salvestusele jäävad isikud;

3.1.12. ameti läbipääsusüsteemi kasutavad isikud

3.1.13. füüsilised isikud, kelle andmeid ametile edastatakse.

4. NÕUSOLEKUPÕHINE ISIKUANDMETE TÖÖTLEMINE

4.1. Kui seaduses, määruses, põhimääruses või lepingus sätestatud ülesannete täitmiseks on vajalik töödelda täiendavaid isikuandmeid, mille töötlemise kohustus ametile ei tulene õigusaktidest peab isik andma kirjaliku nõusoleku oma isikuandmete töötlemiseks.

4.2. Nõusolek peab olema vabatahtlik, ning kirjalikku taasesitamist võimaldavas vormis.

4.3. Enne andmesubjektilt isikuandmete töötlemiseks nõusoleku saamist peab andmesubjektile teatavaks tegema:

4.3.1. vastutava töötleja ja tema kontaktandmed;

4.3.2. töötlemise eesmärgid ja õiguslikud alused;

4.3.3. isikuandmete säilitamise ajavahemiku;

4.3.4. andmesubjektil on õigus taotleda juurdepääsu oma isikuandmetele, nõuda isikuandmete parandamist, kustutamist, töötlemise piiramist ning antud nõusolek igal ajal tagasi võtta;

4.3.5. andmesubjektil on õigus esitada vastuväiteid isikuandmete töötlemise osas ning kaebus järelevalveasutusele (AKI).

4.4. Andmesubjekt saab nõusoleku isikuandmete töötlemiseks anda vaid enda, oma alaealiste laste ning piiratud teovõimega isikute suhtes, kelle eestkostja ta on.

4.5. Kui isikuandmete töötlemisel on mitu eesmärki, tuleb iga töötlemise eesmärgi osas anda eraldi nõusolek.

4.6. Kui isikuandmete töötlemine põhineb nõusolekul, on andmesubjektil õigus nõusolek igal ajal tagasi võtta.

4.7. Amet vastutava töötlejana peab tõendama, et andmesubjekt on andnud nõusoleku oma isikuandmete töötlemiseks. Isikuandmete töötlemise nõusolek registreeritakse dokumendihaldussüsteemis.

5. ANDMESUBJEKTI ÕIGUSED ISIKUANDMETE TÖÖTLEMISEL

5.1. Andmesubjektil õigus saada teada, milliseid isikuandmeid tema kohta kogutakse ja on kogutud, millisel eesmärgil ning millisele seadusele või muule õigusaktile tuginedes tema andmeid töödeldakse ja millistele isikutele või organisatsioonidele on tema isikuandmeid edastatud. Andmesubjektile tuleb võimaldada isikuandmetega tutvumist 30 päeva jooksul alates vastava taotluse esitamisest.

5.2. Andmesubjektil on õigus andmete töötlemiseks nõusolek anda – nõusolek antakse koheselt andmete kogumisel, kui andmeid kogutakse otse andmesubjektilt.

5.3. Andmesubjektil on õigus andmete töötlemiseks antud nõusolek tagasi võtta – nõusoleku alusel toimunud isikuandmete töötlemine tuleb lõpetada koheselt, ilma viivituseta, kuid mitte hiljem kui 30 päeva jooksul.

5.4. Õiguste nõudmine ei tohi andmesubjektile negatiivseid tagajärgi tuua.

5.5. Isikuandmed väljastatakse võimaluse korral andmesubjekti soovitud viisil.

5.6. Isikuandmete väljastamisel peab amet olema veendunud, et tegemist on just selle isikuga, kellel on õigus vastavaid andmeid saada. Seetõttu peab andmete taotleja vajadusel oma isikusamasust või andmete taotlemise õigust tõendama.

5.7. Isikuandmete töötleja on kohustatud põhjendama andmete väljastamisest või teabe andmisest keeldumist. Andmete või teabe andmisest keeldumise otsusest teavitab isikuandmete töötleja andmesubjekti avalduse saamise päevale järgneva viie tööpäeva jooksul.

5.8. Töötlejal on õigus keelduda andmesubjektile teabe edastamisest kui see võib:

5.8.1. kahjustada teise isiku õigusi ja vabadusi;

5.8.2. takistada kuriteo tõkestamist või kurjategija tabamist;

5.8.3. raskendada kriminaalmenetluses tõe väljaselgitamist.

5.9. Andmesubjektil on õigus oma isikuandmete töötlejalt nõuda ebaõigete isikuandmete parandamist.

5.10. Kui isikuandmete töötlemine ei ole seaduse alusel lubatud, on andmesubjektil õigus nõuda:

5.10.1. isikuandmete töötlemise lõpetamist;

5.10.2. isikuandmete avalikustamise või neile juurdepääsu võimaldamise lõpetamist;

5.10.3. kogutud isikuandmete kustutamist või sulgemist.

6. JUURDEPÄÄS ISIKUANDMETELE

6.1. Juurdepääs isikuandmeid sisaldavale andmekogule või infosüsteemile antakse ameti teenistujale ametikoha ülesannete täitmiseks vajalikus ulatuses.

6.2. Juurdepääs peatükis 4. välja toodud isikute isikuandmetele võib ameti teenistujal olla vaid oma ametikoha ülesannete täitmiseks vajalikus ulatuses.

6.3. Teenuste omanikud, andmete ja andmekogude omanikud on kohustatud kontrollima, kas isikuandmeid sisaldavatesse andmekogudesse ja infosüsteemidesse juurdepääsu omavatel isikutel on selleks ametikohajärgne vajadus.

6.4. Ametikoha vahetamisel on kohustus üle vaadata isiku kontod ning juurdepääsuõigused andmekogudes ja infosüsteemides, et välistada õigustamata juurdepääsu isikuandmetele.

6.5. Ametis dokumendi loomisel ja registreerimisel on kohustus pöörata tähelepanu dokumendis sisalduvale teabele. Vastavalt dokumendis sisalduvatele isikuandmetele tuleb juurdepääsupiirangu määramisel ja dokumendi märgistamisel lähtuda avaliku teabe seaduses sätestatud alustest.

6.6. Ameti siseveebis olevad isikuandmed on mõeldud kasutamiseks asutusesiseselt.

6.7. Käesoleva peatüki punktides 6.1 – 6.3 nimetatud õigused ei kehti piiramatult, vaid lähtuda tuleb ka teistest seadustest tulenevatest kohustustest ja piirangutest.

6.8 Käesolevat korda ei kohaldata, kui:

6.8.1. tegu on juriidilise isiku või asutuse andmetega;

6.8.2. teave ei võimalda isikut mõistlike pingutustega tuvastada;

6.9. Kui andmed ei ole kogutud andmesubjektilt endalt, ei pea talle isikuandmete töötlemise kohta teada andma juhul kui:

6.9.1. andmete töötlemine on ette nähtud õigusaktides;

6.9.2. teabe esitamine on võimatu või see nõuab ebaproportsionaalseid jõupingutusi ning amet on kasutusele võtnud meetmed isiku huvide kaitseks;

6.9.3. kui õigusaktide alusel on kohustus andmeid salajas hoida.

7. ISIKUANDMETE TÖÖTLEMISEGA SEOTUD PÖÖRDUMISED

7.1. Ametile saabunud isikuandmete töötlemisega seotud kirjalikud pöördumised registreeritakse dokumendihaldussüsteemis, vajadusel lisatakse juurdepääsupiirang ja suunatakse menetlemiseks ameti struktuuriüksusele.

7.2. Isikuandmete edastamisel tuleb järgida alati minimaalsuse põhimõtet. See tähendab, et vastuvõtjale edastatakse vaid need isikuandmed, mis on andmete kogumise ja edastamise eesmärki silmas pidades õigustatud ja vajalikud.

7.3. Andmesubjekti poolt isiklikult esitatud ja isikuandmete töötlemist puudutavad taotlused tuleb vormistada kirjalikult. Andmesubjektile tuleb selgitada, millise tähtaja jooksul amet isiku pöördumisele vastab.

7.4. Eraisikutega peetav kirjavahetus on üldjuhul juurdepääsupiiranguga, mille alus ja periood märgitakse dokumendiregistrisse.

7.5. Isikuandmete töötlemisega seotud pöördumise puhul, milles küsitakse teavet kolmanda isiku kohta, informeeritakse esitajat, et küsitud teabele ei ole võimalik juurdepääsu võimaldada, välja arvatud juhul, kui:

7.5.1. teabe edastamiseks on olemas seaduslik alus;

7.5.2. teave on seotud poolelioleva kohtumenetluse, väärteomenetluse või haldusmenetlusega;

7.5.3. teabe edastamise aluseks on leping või koostöökokkulepe või isik on andnud loa enda andmete edastamiseks.

7.6. Kolmandatele riikidele andmete edastamiseks peab riik, kuhu andmeid edastada soovitakse, olema Euroopa Liidu poolt loetud piisava kaitsetasemega riigiks, edastamine peab olema seotud rahvusvahelise sõjalise koostöö, välislepingute või rahvusvaheliste ülesannete täitmisega.

7.7. Isikuandmete edastamine kolmandatesse riikidesse peab toimuma turvaliselt ja kontrollitud kanalite kaudu, lähtudes andmete edastamisel minimaalsuse printsiibist. Elektrooniliste sidekanalite kaudu edastatavad dokumendid peavad olema kaitstud kas turvalise parooliga, või olema krüpteeritud.

7.8 Isikuandmeid sisaldavate dokumentide edastamine teistele riigiasutustele peab toimuma turvaliselt: edastades dokumente dokumendihaldussüsteemis, e-posti teel krüpteeritult, kasutades tähitud posti, kullerit või muud turvalist viisi.

7.9. Kaitseministeeriumi haldusalasisene isikuandmete edastamine peab vastama isikuandmete kaitse reeglitele, teabe edastamiseks tuleb kasutada turvalisi kanaleid ja vahendeid. **Eriligiilisi isikuandmeid edastatakse ainult krüpteeritult.**

7.10. Isikuandmeid sisaldavate dokumentide edastamine ameti lepingupartneritele peab toimuma vastavalt lepingus sätestatud nõuetele. Elektrooniliste sidekanalite kaudu edastatavad dokumendid peavad olema parooliga kaitstud, krüpteeritud või edastatud mõnel muul turvalisel viisil.

8. TÖÖTLEJA KOHUSTUSED

8.1. Amet, kui isikuandmete töötleja kohustub:

8.1.1. tagama isikuandmete töötlemise korralduse ja selle kooskõla õigusaktidega, sealhulgas isikuandmete kaitse põhimõtete järgimise;

8.1.2. avalikustama ameti välisveebis ja siseportaalis teabe isikuandmete töötlemise kohta ametis;

8.1.3. teavitama andmesubjekti isikuandmete töötlemisest, välja arvatud juhul, kui andmeid töödeldakse seaduse alusel või kui andmesubjekt on ise andmete töötlemiseks nõusoleku andnud;

8.1.4. tagama isikuandmeid töötlevatele ameti andmetöötlejatele isikuandmete töötlemise ja kaitse alase juhendamise;

8.1.5. isikuandmete töötlemisel rakendama vaikimisi ja lõimitud isikandmete kaitse põhimõtteid;

8.1.6. isikuandmete kaitseks kasutama asjakohaseid, nii organisatsioonilisi, füüsilisi kui ka infotehnoloogilisi turvameetmeid, selleks amet vastavalt vajadusele:

8.1.6.1 kustutab, hävitab või piirab mõistliku aja jooksul eesmärkide saavutamiseks mittevajalikud isikuandmed;

8.1.6.2. tagab isikuandmeid töötlevate süsteemide ja teenuste tervikluse, käideldavuse ja konfidentsiaalsuse;

8.1.6.3. pseudonümiseerib ja krüpteerib isikuandmed;

8.1.6.4. vahejuhtumite korral taastab isikuandmete kättesaadavuse õigeaegselt;

8.1.6.5. testib tehniliste ja korralduslike meetmete tõhusust korrapäraselt;

8.1.6.6. tagab võimalused ja tehnilised lahendused teabe turvaliseks ja lõplikuks kustutamiseks säilitusmeediumi loetamatuks muutmise, füüsilise hävitamise või ülekirjutamise teel.

8.1.7. Pidama elektroonilist isikuandmete töötlemise ülevaadet, mille eesmärgiks on koondada teave ametis tehtavate isikuandmete töötlemise toimingute kohta;

8.1.8. Pidama automatiseeritud viisil tehtavate isikuandmete töötlemise toimingute kohta logisid, mis hõlmavad kogumist, muutmist, lugemist, avalikustamist, edastamist, ühendamist ja kustutamist. Andmekogude ja infosüsteemide eest vastutavad ameti struktuuriüksused või teenuste omanikud on kohustatud koostöös kaitseväe küberväejuhatusega kehtestama logikirjete säilitamise tähtajad ning reeglid logide kontrollimiseks ja nendega tutvumiseks.

8.2. Ameti teenistujad on isikuandmete töötlemisel kohustatud:

8.2.1. kustutama tema kasutusse antud e-postkastist isikuandmeid sisaldavad e-kirjad, mille puhul on isikuandmete töötlemise eesmärk täidetud ning puudub edasine vajadus kirju säilitada;

8.2.2. kustutamiseks või hävitamiseks mõeldud teabe turvaliselt ja lõplikult kustutama või hävitama teabekandja loetamatuks muutmise, füüsilise hävitamise või ülekirjutamise teel;

8.2.3. kustutama isiklikelt võrguketastelt ning oma tööarvutist isikuandmeid sisaldavad failid, mille puhul puudub õiguslik alus nende töötlemiseks;

8.2.4. hävitama isikuandmeid sisaldavad paberkandjal dokumendid, mille puhul ei ole enam edasise töötlemise vajadust ning mida ei ole vaja säilitada;

8.2.5. isikuandmete edastamisel kasutama turvalisi edastusviise ja vahendeid;

8.2.6. dokumendi koostamisel ja registreerimisel hindama, kas dokumendis sisalduv teave on juurdepääsupiiranguga (AK) Avaliku teabe seaduse alusel. Kui dokumendis sisalduv teave on juurdepääsupiiranguga, siis on dokumendi koostajal kohustus dokument vastavalt märgistada;

8.2.7. teavitama isikuandmete töötlemise rikkumisega seotud intsidentidest vahetut juhti ja ameti andmekaitse valdkonna eest vastutatavat isikut;

8.2.8. ebaseaduslikult või ebaõigelt edastatud isikuandmete puhul teavitama sellest saatjat ja vastuvõtjat ning struktuuriüksuse juhti ja ameti andmekaitse valdkonna eest vastutavat isikut;

8.2.9. hoidma konfidentsiaalsena tööülesannete täitmisel teatavaks saanud teavet isikuandmete kohta ka pärast isikuandmete töötlemisega seotud tööülesannete täitmist ning töö- või teenistussuhte lõppemist.

8.3. Tagamaks isikuandmete kaitse põhimõtete järgimiseks infotehnoloogilise võimekuse ning vajalike infotehnoloogiliste turvameetmete olemasolu, on vajalik:

8.3.1. vähemalt üks kord aastas hinnata ja kontrollida, kas isikuandmete töötlemine kasutusel olevates infosüsteemides ja andmekogudes vastab turvalisuse nõuetele;

8.3.2. puuduste esinemisel planeerib infoturbe eest vastutav isik parendamistöid või süsteemide muutmist.

9. ISIKUANDMETE TÖÖTLEMISEGA SEOTUD TURVALISUS JA RISKID

9.1. Amet töötleb isikuandmeid valdavalt asutusesiseseks kasutamiseks mõeldud teabe töötlussüsteemis, lisaks salastatud teabe töötlussüsteemis (salastatud teabe töötlussüsteemi isikuandmete kaitse juhendis ei käsitleta).

9.2. Juurdepääsu isikuandmetele saavad vaid ameti andmetöötlejad, kellel on selleks vajalik õigus ja ainult selles ulatuses, mis on vajalik eesmärgi saavutamiseks.

9.3. Juhul, kui isikuandmetega seonduvalt toimub mistahes intsident, tuleb koheselt tarvitusele võtta kõik vajalikud meetmed tagajärgede leevendamiseks ning tulevikus sarnaste riskide maandamiseks.

9.4. Ameti struktuuriüksused on kohustatud rakendama isikuandmete kaitseks infotehnoloogilisi, füüsilisi ja organisatsioonilisi turvameetmeid, informeerima üldistest turvameetmetest, nende rakendamisest ja isikuandmete kaitsemeetmete kasutamise kohustusest ameti kõiki teenistujaid.

9.5. Isikuandmete töötlemistoimingud võivad olla seotud inimestest, tehnoloogiast, tööprotsessidest tulenevate riskidega, mille käigus võib andmesubjektile tekkida füüsiline, varaline või mittevaraline kahju.

10. MÕJUHINNANG

10.1. Olemasolevate ning planeeritavate isikuandmete töötlemisega seotud andmekogude, infosüsteemide või uue tarkvara kasutuselevõtmisel on kohustus hinnata, kas kasutamisel võib tõenäoliselt tekkida oht isikuandmete töötlemisel.

10.2. Mõjuhinnangu protsessi tuleb kaasata andmekaitse eest vastutav isik, kes veendub planeeritava lahenduse isikuandmete kaitse nõuetele vastavusest.

10.3. Mõjuhinnang tuleb alati läbi viia kui:

10.3.1. töödeldakse suurt hulka isikuandmeid, mis võivad mõjutada paljusid andmesubjekte;

10.3.2. kasutusele võetakse eriliiki isikuandmete töötlemisega seotud süsteem, muudetakse kasutusel olevaid isikuandmete töötlemisega seotud süsteeme või muudetakse isikuandmete töötlemise protsesse.

10.4. Mõjuhinnangu läbiviimise alustamisest on kohustus teavitada andmekaiste eest vastutavat isikut.

10.5. Mõjuhinnang peab olema koostatud ühtselt arusaadavas sõnastuses.

10.6. Mõjuhinnangu läbiviimise käigus hinnatakse ja analüüsitakse isikuandmete töötlemisega kaasnevaid riske koos riskide maandamise võimalustega, et hinnata, kas rakendatavad meetmed on piisavad ohtude täielikuks maandamiseks või viimiseks aktsepteeritavale tasemele.

10.7. Mõjuhinnangu läbiviimisel peab arvestama kehtivaid andmekaitse põhimõtted, õigusakte haldusalaüleseid juhendeid ja kordasid, asjassepuutuvaid direktiive ja määruseid ning varasemat praktikat.

11. ISIKUANDMETE TÖÖTLEMISEGA SEOTUD RIKKUMISED JA TEAVITAMINE

11.1. Isikuandmete töötlemisega seotud turvalisuse nõuete rikkumine on isikuandmetele autoriseerimata juurdepääsu või juurdepääsu võimaluse võimaldamine, isikuandmete loata edastamine, kustutamine, hävitamine, muutmine või kaotsiminek.

11.2. Amet registreerib rikkumised isikuandmete töötlemise rikkumiste registris, sealhulgas rikkumise asjaolud, mõju ning parandusmeetmeid.

11.3. Rikkumise avastamise korral on ameti teenistuja kohustatud sellest teavitama koheselt oma struktuuriüksuse juhti ja ameti andmekaitse eest vastutavat isikut.

11.4. Andmekaitse eest vastutav isik koostöös ameti infoturbe juhi, struktuuriüksuse juhi ja andmetöötlejaga on kohustatud võtma kasutusele meetmed, et rikkumine koheselt lõpetada ja selgitada välja rikkumisega seotud asjaolud.

11.5. Esmased toimingud peab läbi viima hiljemalt 48 tunni jooksul peale rikkumisteate saamist.

11.6. Ametis tuvastatud rikkumise puhul on rikkumise avastanud struktuuriüksusel kohustus võtta viivitamata kasutusele meetmed tagajärgede leevendamiseks ning piirata andmete kasutust kuni rikkumise põhjuste ja kaasneva ohu ulatuse selgumiseni.

11.7. Kui isikuandmetega seotud rikkumine kujutab endast tõenäolist ohtu andmesubjekti õigustele ja vabadustele, teavitab ameti andmekaitse eest vastutav isik hiljemalt 72 tunni jooksul pärast rikkumisest teada saamist Andmekaitse Inspektsiooni.

11.8. Kui rikkumise tulemusena tekib andmesubjekti õigustele ja vabadustele tõenäoliselt suur oht, teavitab ameti andmekaitse eest vastutav isik andmesubjekti, mis võimaldab andmesubjektil endal võtta vajalikke ettevaatusabinõusid olukorra leevendamiseks.