TÖÖ PROGRAMM	Kuupäev: 18.12.2025	Koostaja: Bernd Rannamägi	Viide: B4-1

Töö nimetus	Isikuandmete kaitse korralduse ülevaade
Töö eesmärk	Selgitada, kuidas on KliM valitsemisalas korraldatud isikuandmete töötlemine. Ülevaade koostatakse koostöös valitsemisala asutuste andmekaitsespetsialistidega (AKS) ning sellega saavutatakse isikuandmete töötleja isikuandmete kaitse turvameetmete alase teadlikkuse tõstmine, mittevastavusega seotud probleemide ennetav lahendamine ning vajadusel ka isikuandmete töötlemise kooskõlla viimine normidega. Samuti valideeritakse isikuandmete töötlemisülevaate koostamise protsessi.
Töö ulatus	Valitsemisala isikuandmete kaitse korraldusest ülevaate koostamisel selgitatakse asutuste tegevusi lähtuvalt Isikuandmete kaitse üldmääruse[1] (GDPR) nõuetest, sh artiklid: 30 (töötlemisülevaade), 24 (vastutava töötleja kohustused) ja 35 (mõjuhinnangud) ning Isikuandmete kaitse seadus (IKS) § 37. Ülevaade hõlmab järgmisi teemasid: välisveebilehe andmekaitsetingimused, koolitused, intsidendihaldus, andmekaitsealased mõjuhinnangud (DPIA), lepingud volitatud töötlejatega, töötlemisülevaate haldamine, sh andmete säilitamise põhimõtted. Ülevaate koostamisel kogutakse asutustelt info kehtivate protsesside, vastutajate ja praktika kohta ning selgitatakse koostöökohti ministeeriumi andmekaitsespetsialistiga isikuandmete töötlemisülevaate koostamisel ja täiendamisel.
Töö ulatuse piirang	Töö iseloomust tulenevalt kirjeldatakse isikuandmete töötlemise olukorda, koondatakse sellekohased faktid ja tuvastatakse võimalikud kitsaskohad, mille kohta tehakse soovitusi. Töös ei hinnata isikuandmete töötlemise vastavust nõuetele.

Töö teema on oluline, sest isikuandmete kaitse on üks inimese põhiõigusi. Kuna isikuandmete töötlemine riivab eraelu puutumatust, peab andmetöötleja tagama kodanikule ligipääsu tema kohta kogutud andmetele ja teabele ning andma selgitusi töötlemise ulatuse, eesmärgi ja õigusliku aluse kohta.

2016. aasta 14. aprillil kiitis Euroopa Parlament heaks Isikuandmete kaitse üldmääruse (inglise keeles General Data Protection Regulation, GDPR) ja tunnistas kehtetuks senini kehtinud andmekaitsedirektiivi[2]. GDPR on otsekohalduv õigusakt, mis koos siseriiklike rakendusaktidega asendas varasema Eesti isikuandmete kaitse seaduse. Määrus jõustus 24.05.2016 ning seda hakati kohaldama alates 25.05.2018 pärast kaheaastast üleminekuaega. Eesti võttis GDPR-i rakendamiseks vastu Isikuandmete kaitse seaduse[3], mis täpsustab ja täiendab üldmääruse riigis kohaldamist.

GDPRi läbivaks eesmärgiks on tugevdada andmetöötlejate (vastutava ja volitatud töötaja) vastutustundlikkust ning ühtlustada andmekaitse reegleid kõigis ELi liikmesriikides. Vastustundlikkuse põhimõte tähendab, et andmetöötlejad peavad olema võimelised aru saama ja **omama täielikku ülevaadet andmetöötluse ahelast ning tagama isikuandmete töötlemise seaduslikkuse[4], proportsionaalsuse[5] ja läbipaistvuse[6]**.

Avaliku sektori asutustel lasub kohustus tagada, et isikuandmete töötlemine on seaduslik, õiglane ja läbipaistev, lähtudes eesmärgipärasuse[7] ja minimaalsuse[8] põhimõtetest. Samuti tuleb rakendada piisavaid turvameetmeid, et vältida volitamata juurdepääsu andmetele, sh isikuandmetele. Isikuandmete töötlemisel peab alati olema õiguslik alus, selle puudumisel rikutakse GDPR-i artikli 5 lõike 1 punktis a sätestatud seaduslikkuse põhimõtet.

[1] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

[2] 24. oktoober 1995 Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.

[3] Isikuandmete kaitse seadus (IKS) kuulutati välja Vabariigi Presidendi 21.12.2018 otsusega nr 367.

[4] **Seaduslikkuse põhimõte**: Isikuandmeid võib töödelda ainult siis, kui selleks on olemas *õiguslik alus* (nt nõusolek, leping, seadusest tulenev kohustus, elulised huvid, avalik ülesanne või õigustatud huvi).

[5] **Proportsionaalsuse põhimõte**: Isikuandmete töötleja peab tagama, et andmete kogumine ja kasutamine on eesmärgiga kooskõlas, vältides liigset sekkumist andmesubjekti õigustesse ning piirdudes üksnes tööalase minimaalse teadmisvajadusega.

[6] **Läbipaistvuse põhimõte**: Isikuandmete töötlemine peab olema inimese jaoks arusaadav, selgelt esitatud ja kergesti kättesaadav. Andmesubjekt peab teadma, kes tema andmeid töötleb, mis eesmärgil, kui kaua ja millised õigused tal on.

[7] **Eesmärgipärasuse põhimõte**: Isikuandmeid võib koguda ja töödelda ainult selgelt määratletud, õiguspärastel ja konkreetsetel eesmärkidel ning neid ei tohi hiljem kasutada viisil, mis ei ole nende algsete eesmärkidega kooskõlas.

[8] **Minimaalsuse põhimõte**. Isikuandmeid tuleb koguda ja töödelda vaid nii palju, kui on vajalik konkreetse ja õiguspärase eesmärgi saavutamiseks.

Justiits- ja Digiministeerium on andmesubjekti isikuandmete töötlemise läbipaistvuse suurendamiseks ja vähendamaks andmesubjekti vajadust saata igale riigiasutusele eraldi päring tema andmete kasutamise kohta, edastanud ministeeriumitele, põhiseaduslike institutsioonidele ja huvigruppidele arvamuse avaldamiseks ning kooskõlastuse saamiseks AvTS muudatuse väljatöötamiskavatsuse[9], millega muutuks andmejälgija[10] kasutamine avalikule sektorile kohustuslikuks.

KliM SAO ei ole varasemalt isikuandmete teemat käsitlenud GDPR-i põhimõtetest lähtudes eraldi audititöö objektina. 2023. aastal viidi läbi audit „Avaliku teabe seaduse nõuete ühetaoline ja seadusega kooskõlas rakendamine“, mille käigus analüüsiti muu hulgas AKS-i alluvussuhteid riigiasutustes. Toimingust nähtus, et AKS-i ametikoha paiknemine eri ministeeriumite/riigiametite struktuuris on erinev. Ka näitasid tulemused, et AKS-i ametikoha paiknemine organisatsioonistruktuuris on erinev, rolli täitjatel oli valdavalt magistrikraad ja õigusalane taust ning rolli täideti sageli koos muude tööülesannetega.

Käesolev töö teostatakse KliM siseauditi osakonna 2025. aasta tööplaani kohaselt nõuandva tööna ja selle laiem eesmärk on anda ülevaade valitsemisala asutuste isikuandmete kaitse korraldusest.

Töös käsitletavad teemad ja küsimused:

1. **KliM-is ja valitsemisala asutustes isikuandmete kaitse korraldusest ülevaate koostamine**. Selleks koondatakse peamised andmed valitsemisala asutuste isikuandmete kaitse korralduse kohta, et koostada asutusepõhine koondülevaade.

   1.1. **Korraldus ja juhendid**. Selgitatakse, kas ja millised dokumendid on loodud ministeeriumis ja allasutustes isikuandmete kaitse korraldamisel. Koondatakse info dokumentide kättesaadavuse ja ajakohastamise kohta ning selgitatakse, kuidas on tagatud nendes toodud põhimõtete tutvustamine teenistujatele, sh kas isikuandmete töötlemise põhimõtted on avalikustatud asutuse välisveebis. Uuritakse, kas asutustel on muresid seoses juhendite rakendamise või ajakohastamisega.

   Alamküsimused:

   - ✓ Millised sisekorrad, juhendid või protseduurid asutuses reguleerivad isikuandmete kaitse tagamist? Kas, milliseid regulatsioone vm kokkuleppeid on loodud eraldi isikuandmete kaitseks?
   - ✓ Millal toimus nende viimane ajakohastamine (kuupäev)?
   - ✓ Kas teenistujatele on juhendid tutvustatud? Kas/ kus on juhendid ja asutuseisesed regulatsioonid leitavad ja kättesaadavad?
   - ✓ Kas ministeeriumi ja allasutuste välisveebis on avaldatud privaatsustingimused või töötlemise põhimõtted?
   - ✓ Kuidas on tagatud nende ajakohastamine (nt regulaarne ülevaatus, vastutaja)?
   - ✓ Kas asutusel on muresid või väljakutseid seoses juhendite rakendamise, kättesaadavuse või ajakohastamisega?

   1.2. **Andmekaitsespetsialisti rolli täitmine** (GDPRi artiklid 37 – 39). Selgitatakse, kas asutuses on AKS määratud, kuidas on korraldatud tema rolli täitmine, tööülesannete jaotus ning sõltumatuse tagamine. Koondatakse info äriregistri andmete õigsuse kohta ja selgitatakse, kas rolli täitmisega seoses on asutuses murekohti.

   Alamküsimused:

   - ✓ Kas asutuses on määratud andmekaitsespetsialist?
   - ✓ Kas asutuses on määratud andmekaitsespetsialisti asendaja (puhkuste jm puudumiste olukorraks)?
   - ✓ Kas äriregistris on kajastatud andmekaitsespetsialisti nimi ja kontaktandmed? Kui äriregistris puudub/ on aegunud info, selgitatakse põhjusi ja koondatakse korrektne rolli täitja info.
   - ✓ Kas asutuse siseveebis on kajastatud AKSi kontaktandmed?
   - ✓ Kuidas toimub asutuses AKS-i määramine (nt lisaülesannete käskkiri, leping, muu)?
   - ✓ Kas ametijuhendis, töölepingus vm AKS-i määramise dokumendis on kirjas AKS-i ülesanded?

[9] Avaliku teabe seaduse muutmise seaduse väljatöötamiskavatsus.

[10] Andmejälgija on teenus, mis võimaldab inimesel riigiportaali **eesti.ee** ja riigiäpi kaudu näha logisid tema isikuandmete töötlemise kohta (st inimesel on võimalik riigiportaalist näha, kes, millal ja miks on riiklikes andmekogudes tema andmeid vaadanud). Hetkel tuleb inimesel oma andmete kasutamise kohta info saamiseks esitada igale asutusele eraldi teabenõude. Andmejälgija automatiseerib selle protsessi.

- ✓ Kui teenistuja täidab AKS rolli lisaülesandena, selgitatakse, millises mahus teenistuja asutuses AKSi rolli täidab?
- ✓ Kelle alluvuses AKS töötab? Kuidas on tagatud AKS-i sõltumatus (nt otsene juurdepääs juhtkonnale, eraldi rollikirjeldus)?
- ✓ Kas asutusel on muresid või väljakutseid AKS-i rolli täitmisega?

1.3. **Töötlemisülevaade** (GDPR artikkel 30). Selgitatakse, kas asutuses on koostatud isikuandmete töötlemise ülevaade (töötlemistoimingute register), millises etapis see on, kuidas on korraldatud selle haldamine ja ajakohastamine ning kes nende tegevuste eest vastutab. Koondatakse info töövahendite, kaasatud üksuste ja ajakava kohta. Uuritakse, kas asutustel on muresid seoses ülevaate koostamise või ajakohasena hoidmisega.

Alamküsimused:

- ✓ **Staatus ja ajakava.** Kas asutusel on isikuandmete töötlemise ülevaade (GDPR artikkel 30)?
  - Kui jah, millal see koostati ja kuidas seda ajakohastatakse (nt sagedus, vastutaja)?
  - Kui ülevaade on koostamisel, millises etapis see praegu on ja mis on planeeritud valmimise tähtaeg?
  - Kui ülevaate koostamist ei ole alustatud, kas on kokku lepitud ajakava ja vastutaja selle koostamiseks?
- ✓ **Vastutajad ja protsess.** Kes vastutab töötlemisülevaate koostamise ja ajakohastamise eest (ametikoht)? Millised üksused või osakonnad on kaasatud ülevaate koostamisse? Milliseid töövahendeid ja protsesse kasutatakse ülevaate haldamiseks (nt Excel, spetsiaalne tarkvara)?
- ✓ **Ülevaate sisu (GDPR-i põhielemendid). Kui asutusel on isikuandmete töötlemisülevaade olemas, kogutakse infot faktide tõendamiseks, mitte hindamiseks, kas asutuse töötlemise ülevaates on kajastatud järgmised elemendid:**
  - Kas on kajastatud andmesubjektide kategooriad (nt töötajad, kliendid, partnerid)?
  - Kas on kajastatud eriliigiliste isikuandmete töötlemine?
  - Kas igale töötlemistoimingule on määratud õiguslik alus?
  - Kas on märgitud andmete säilitustähtajad?
  - Kas on kirjeldatud turvameetmete üldine raamistik (GDPR artikkel 32)?
- ✓ Kas asutusel on muresid või väljakutseid seoses töötlemisülevaate koostamise, ajakohastamise või vastutuse määramisega?

1.4. **Veebilehe andmekaitsetingimused.** Selgitatakse, kuidas on korraldatud asutuse veebilehel avaldatud privaatsustingimuste ja isikuandmete töötlemise põhimõtete ülevaatus ja ajakohastamine. Koondatakse info vastutaja, ülevaatamise sageduse ja viimase uuenduse kohta. Uuritakse, kas asutustel on muresid seoses veebisisu ajakohasena hoidmisega.

Alamküsimused:

- ✓ Kas asutuse veebilehel on avaldatud privaatsustingimused (GDPRi artiklid 12-14) või isikuandmete töötlemise põhimõtted? Kui jah, millal toimus nende viimane ülevaatus või ajakohastamine?
- ✓ Kui tihti on kokku lepitud nende ülevaatamise sagedus (nt kord aastas, vastavalt vajadusele)?
- ✓ Kes vastutab veebilehe andmekaitsetingimuste ajakohastamise eest (ametikoht)?
- ✓ Kas asutusel on muresid või väljakutseid seoses veebilehe andmekaitsetingimuste ajakohasena hoidmisega?

1.5. **Koolitused.** Selgitatakse, kas ja kuidas on korraldatud isikuandmete kaitse alased koolitused valitsemisala asutustes. Koondatakse info koolituste regulaarsuse, sihtrühmade ja osalejate kohta. Uuritakse, kas asutustel on muresid seoses koolituste korraldamise või töötajate teadlikkuse tõstmisega.

Alamküsimused:

- ✓ Kas asutuses pakutakse isikuandmete kaitse teemal koolitusi? Kui jah, kui tihti neid korraldatakse (nt kord aastas, vastavalt vajadusele)? Koondatakse andmed viimase kahe aasta koolituste kohta: kuupäev, osalejate arv, sihtrühm (nt juhtkond, kõik töötajad, uued töötajad).
- ✓ Kas koolituste sisu hõlmab GDPR-i ja IKS-i nõudeid?
- ✓ Kas koolituste korraldamise eest vastutab andmekaitsespetsialist või muu ametikoht?
- ✓ Kas asutusel on muresid või väljakutseid seoses koolituste korraldamise, osalemise või töötajate teadlikkuse tõstmisega?

1.6. **Intsidendihaldus.** Selgitatakse, kuidas on korraldatud isikuandmetega seotud intsidendihaldus valitsemisala asutustes. Koondatakse info vastava korra, vastutaja ja intsidendihalduse protsessi kohta. Uuritakse, kas asutustel on muresid seoses intsidendihalduse rakendamisega.

Alamküsimused:

- ✓ Kas asutuses on kehtestatud kord või juhend isikuandmetega seotud intsidendi käsitlemiseks?
- ✓ Kes vastutab intsidendihalduse eest (ametikoht)?
- ✓ Kuidas toimub intsidendi tuvastamine, dokumenteerimine ja teavitamine (nt AKI-le)?
- ✓ Kas on määratletud ajakava ja protsess intsidendi lahendamiseks[11] (GDPRi artiklid 33 - 34)?
- ✓ Koondatakse info perioodil 01.07.2023–31.12.2025 toimunud andmekaitseintsidentidest: intsidendi lühikirjeldus, rakendatud meetmed, kas teavitati AKIt ja kui insident hinnati kõrgendatud ohuks, kas teavitati ka andmesubjekti.
- ✓ Kas asutusel on muresid või väljakutseid seoses intsidendihalduse korraldamisega?

1.7. **Mõjuhinnangud.** Selgitatakse, kas ja kuidas on korraldatud andmekaitse mõjuhinnangute (Data Protection Impact Assessment, DPIA) läbiviimine valitsemisala asutustes. Eesmärk on selgitada, kas hinnangute tegemise vajadus on läbi mõeldud, kas protsess on kehtestatud ja kas hinnanguid on koostatud. Koondatakse info vastutuse, dokumenteerimise ja peamiste väljakutsete kohta.

Alamküsimused:

- ✓ Kas asutuses on kehtestatud kord või juhend andmekaitse mõjuhinnangu (DPIA) läbiviimiseks?
- ✓ Kui protsessi ei ole kehtestatud, kas hinnangute vajadus on üldse läbi mõeldud (nt riskianalüüs, GDPR art 35 nõuded)?
- ✓ Kas asutus on viimase 2 aasta jooksul koostanud andmekaitsealaseid mõjuhinnanguid? Kui jah, millal ja millistel juhtudel hinnangud koostati (nt uue IT-süsteemi juurutamisel, uue teenuse käivitamisel, kõrge riskiga töötlemisel)? Kes osales hinnangute koostamisel (ametikohtade kaupa)?
- ✓ Kus on kirjeldatud andmekaitsealaste mõjuhinnangute koostamise protsess (nt sisejuhend, andmekaitse kord) ja kes vastutab mõjuhinnangute läbiviimise eest (ametikoht)?
- ✓ Kas hinnanguid ajakohastatakse?
- ✓ Koondatakse info perioodil 01.07.2023–31.12.2025 koostatud mõjuhinnangute kohta: hinnangu koostamise kuupäev, eesmärk, peamised riskid ja rakendatud leevendusmeetmed.
- ✓ Kas asutusel on muresid või väljakutseid seoses mõjuhinnangute koostamise, ajakohastamise või rakendamisega?

1.8. **Lepingute ja üldtingimuste kontroll**. Selgitakse, kas asutus kontrollib volitatud töötlejate vastavust GDPRile nii enne lepingu sõlmimist kui ka lepingu kehtivuse ajal, rakendades ühtseid protsesse, regulaarset järelevalvet ja selgeid sanktsioonimehhanisme.

Alamküsimused:

- ✓ Kas asutuses on kehtestatud standardne protsess või üldtingimused, mida rakendatakse kõigi volitatud töötlejate lepingute puhul (nt DPA tüüptingimused)? Kas lepingutes on selgelt määratletud:

[11] AKS teavitab isikuandmetega seotud rikkumisest AKI-t 72 tunni jooksul. AKI-le esitatav rikkumisteade peab kirjeldama rikkumise olemust, mõjutatud isikuandmete kategooriaid, hinnangut rikkumise tagajärgedele ning meetmeid, mida on rakendatud olukorra lahendamiseks. Kui rikkumise tulemusena tekib inimeste õigustele ja vabadustele tõenäoliselt suur oht, peab AKS põhjendamatu viivituseta sellest teavitama ka andmesubjekti.

- isikuandmete töötlemise eesmärk ja ulatus,
- turvameetmed (GDPR art 32),
- alamtöötlejate kaasamise tingimused,
- andmete tagastamise või kustutamise kord lepingu lõppedes?

✓ Kas andmekaitsespetsialist või vastutav töötleja osaleb **hangete alusdokumentide ja lepingute kooskõlastusringis**, et tagada GDPR nõuete järgimine (GDPRi artikkel 38[12])?

✓ Volitatud töötlejate ja alamtöötlejate kontrolli osas selgitame (GDPRi artikkel 28)[13]

- Kas asutus kontrollib enne lepingu sõlmimist volitatud töötleja vastavust GDPR-ile (nt due diligence)?
- Kas on kehtestatud protsess, kuidas volitatud töötlejad taotlevad luba alamtöötlejate kaasamiseks ja kuidas seda dokumenteeritakse?

✓ Vastavuse tõendamisel ja järelevalves selgitame (GDPRi artikkel 28)[14]

- Kas asutus teeb volitatud töötlejate kohta regulaarseid kontrolle või auditeid? Kui jah, millise sagedusega ja kuidas tulemusi dokumenteeritakse?
- Kas on olemas mehhanism, kuidas reageeritakse volitatud töötleja rikkumistele (nt lepingu lõpetamine, sanktsioonid)?

2. <u>Koostöö isikuandmete töötlemisülevaate koostamise protsessis</u>

Selgitatakse koostöökohti ministeeriumi andmekaitsespetsialistiga isikuandmete töötlemisülevaate koostamisel ja täiendamisel.

2.1. Osakonnapõhiste kaardistuste valideerimine ja täiendamine. Kontrollitakse olemasolevaid KliMi osakonnapõhiseid isikuandmete töötlemise kaardistusi ning vajadusel täiendatakse. Selleks viiakse läbi intervjuud kõigi KliMi tugiosakondadega (v.a SAO) ja kolme sisuosakonnaga, kaasates KliMi andmekaitsespetsialisti (AKS). Intervjuude eesmärk on tuvastada, kas lisaks olemasolevale infole on veel töötlemistoiminguid, mis tuleb ülevaatesse lisada.

2.2. Töötlemisülevaate koostamise toetamine. Abistatakse KliMi andmekaitsespetsialisti töötlemisülevaate korrastamisel ja lõpliku versiooni koostamisel, tagades, et ülevaade vastab GDPR artikli 30 nõuetele ning kajastab kõiki töötlemistoiminguid, õiguslikke aluseid, säilitustähtaegu ja turvameetmeid.

2.3. Kitsaskohtade ja riskide tuvastamine. Intervjuude ja ülevaate koostamise käigus tuvastatakse võimalikud kitsaskohad või riskid (nt puuduvad protsessid, ebapiisavad juhised, lepingute kontrolli puudumine). Vajadusel tehakse ettepanekud protsesside täiendamiseks ja parendamiseks.

3. <u>Vastavalt vajadusele valitsmisalaväliste praktikate uurimine</u>

Vajalikud dokumendid / info / ligipääsud vms:

- Valdkonda reguleerivad dokumendid, sh asutuste sisekorrad, valdkondlikud juhendmaterjalid.
- Ligipääs asutuse koostatud isikuandmete töötlemise ülevaatele (GDPR art 30).
- Ligipääs perioodil 01.07.2023–31.12.2023 toimunud isikuandmete teemaliste koolituste andmetele (kuupäev, osalejate arv, sihtrühm).
- Kliimaministeeriumi lennundus-, merendus- ja rohereformi osakonna isikuandmete töötlemistoimingute info.
- Viited kehtivatele andmekaitse mõjuhinnangute (DPIA) dokumentidele, kui need on koostatud.
- Näited volitatud töötlejatega sõlmitud andmetöötluslepingutest (DPA) ja nende ajakohastamise protsess.

[12] GDPRi artikkel 38 sätestab, et andmekaitsespetsialist peab olema õigeaegselt ja asjakohaselt kaasatud kõigisse isikuandmete kaitsega seotud küsimustesse.

[13] GDPRi artikkel 28 lg 1 ja 2 sätestavad, et vastutav töötleja võib kasutada ainult neid volitatud töötlejaid, kes pakuvad piisavaid garantiisid, et rakendada asjakohaseid tehnilisi ja organisatsioonilisi meetmeid, mis vastavad GDPRi nõuetele ning volitatud töötleja ei tohi kaasata alamtöötlejat ilma vastutava töötleja eelneva kirjaliku loata.

[14] GDPRi artikkel 28 lg 3 ja 4 sätestavad, et lepingus peavad olema kirjas tingimused, mis annavad vastutavale töötlejale õiguse ja võimaluse kontrollida volitatud töötleja tegevust, sh auditeerida ja nõuda tõendamist.

- Info asutuses toimunud isikuandmete intsidentidest perioodil 01.07.2023–31.12.2025
- Asutuse intsidendihalduse korrad või protsessi kirjeldused;
- Kasutuses olevad töövahendid töötlemisülevaate haldamiseks (Excel, tarkvara).

Peamised valdkonnaga seotud õigusaktid / juhendid

- Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 – isikuandmete kaitse üldmäärus (GDPR).
- Isikuandmete kaitse seadus (IKS).
- Avaliku teabe seadus (AvTS).
- Andmekaitse Inspektsiooni „Isikuandmete töötlejate üldjuhend“ (viimati uuendatud 19.03.2019).
- Asutuste kehtestatud isikuandmete töötlemise sisekorrad.

Töö teostamise ajakava:

- Toiminguid teostame jaanuar – aprill 2026.
- Ülevaate eelnõu planeerime esitada mais 2026.
- Ülevaate eelnõu esitatakse asutustele faktivigade kontrolliks.
- Allkirjastatud ülevaate edastamine ja lõplike tulemuste tutvustamine on planeeritud eelnõu kooskõlastamise järgselt orienteeruvalt juunis 2026. a.

Töö juht: Bernd Rannamägi, *siseaudiitor*
/*allkirjastatud digitaalselt*/
Siseauditeerimise eest vastutav isik (AVI): Maarja Kilter, *siseauditi osakonna juhataja*
/*allkirjastatud digitaalselt*/

Isikuandmete kaitse õigusraamistik on viimastel aastatel muutunud keerukamaks ning kiire infotehnoloogiline areng on toonud kaasa uusi võimalusi ja riske. Avaliku sektori asutused vajavad üha enam andmekaitsealast kompetentsi, et tagada vastavus kehtivatele nõuetele ja vältida rikkumisi.

Andmekaitsespetsialisti (AKS) roll ja määramise kohustus

Üldmääruse artiklis 37 on sätestatud AKSi mõiste[15] ja tema määramise kohustus. AKS-i määramise kohustus on avaliku sektori asutusel või organil, andmetöötlejatel, kelle põhitegevuseks on ulatuslik andmesubjektide korrapärane ja süstemaatiline jälgimine, andmetöötlejad, kelle põhitegevuseks on eriliiki isikuandmete töötlemine või süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine.

Üldmäärusest tuleneva kohustuse täitmiseks edastas KliMi strateegia- ja innovatsiooni asekantsler 20.03.2024 valitsemisala asutuste juhtidele (v.a TRAM) e-kirja juhisega määrata AKSi rolli täitja, määratleda tema tööaja osakaal ning kanda äriregistrisse asutuse AKSi kontaktandmed (AKSi rollitäitja ees- ja perekonnanimi, e-posti aadress).

AKSi põhiülesanded GDPR-ist ja IKS-ist tulenevalt:

- olla andmesubjektidele kontaktisikuks kõigis küsimustes, mis on seotud nende isikuandmete töötlemise ja nende andmekaitseliste õiguste kasutamisega;
- teavitada ja nõustada oma organisatsiooni (vajadusel ka selle partnerite) juhtkonda ning personali andmekaitse alal;
- jälgida andmekaitsenormide rakendamist, sealhulgas vastutusvaldkondade jaotamist, personali teadlikkust ja koolitamist, ning andmekaitselist auditeerimist;
- anda nõu seoses andmekaitsealase mõjuhinnanguga ning jälgida selle toimimist;
- teha koostööd Andmekaitse Inspektsiooniga, olles tööandja kontaktisikuks.

Töötlemisülevaate (artikkel 30) olulisus

Kuna üldmääruse ja direktiivi üks läbivaid põhimõtteid on andmetöötleja vastutus, st andmetöötleja vastutab inimeste suhtes seadusliku, õiglase ning läbipaistva andmetöötluse korraldamise eest, ei ole seda kõike võimalik teha, kui andmetöötlejal ei ole täielikku ülevaadet asutuse andmetöötlusest. Seetõttu kohustab üldmääruse artikkel 30 organisatsioone, kes töötlevad isikuandmeid, sõltumata organisatsiooni suurusest, pidama isikuandmete töötlemisülevaadet (andmetöötlustoimingute registrit[16]).

Isikuandmete töötlemise ülevaade on asutuse andmekaitsespetsialisti jaoks keskne töövahend, mis koondab süsteemselt teabe isikuandmete kogumise, kasutamise, edastamise ja säilitamise praktikate kohta. Ülevaade võimaldab isikul hinnata töötlemise vastavust kehtivatele õigusaktidele, tuvastada võimalikke riske ning kavandada asjakohaseid turvameetmeid ja koolitusi. Samuti loob see aluse tõhusaks suhtluseks järelevalveasutustega ning tagab valmisoleku vastata andmesubjektide päringutele. Kokkuvõttes toetab ülevaade andmekaitsespetsialisti tööd, muutes selle läbipaistvamaks, süsteemsemaks ja tõhusamaks.

Isikuandmete töötlemisülevaadet peab pidama kirjalikus või elektroonilises vormis ning see võib olla nii ühes kui mitmes dokumendis. Kuna AKI võib andmetöötlejalt ülevaate välja nõuda, peab ülevaate elektrooniline vorming võimaldama selle kopeerimist ja avamist.

GDPR nõuab, et töötlemisülevaates kajastuks:

- vastutava töötleja ning asjakohasel juhul kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed;
- töötlemise eesmärgid – milleks asutus isikuandmeid kasutab;
- andmesubjektide kategooriate ja isikuandmete liikide kirjeldus;
- vastuvõtjate kategooriad, kellele isikuandmeid on avalikustatud või avalikustatakse, sealhulgas kolmandates riikides olevad vastuvõtjad ja rahvusvahelised organisatsioonid;
- kui isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis andmed selle kohta koos asjaomase kolmanda riigi või rahvusvahelise organisatsiooni nimega, ning juhul, kui tegemist

[15] **AKS on isik**, kes täidab asutuses nö „tõlgi“ rolli – ta peab oskama andmekaitset selgitada nendele, kes ei ole selle ala spetsialistid. Lihtsustatult väljendades peab selle rolli kandja olema kogu asutusele (sh ministeeriumi valitsemisalale) kontaktiks/nõunikuks IKÜM, isikuandmete kaitse seaduse (IKS) ja ka avaliku teabe seadusega (AvTS) seonduvate küsimuste osas.

[16] Andmetöötlusregister on ülevaade dokumendi või infosüsteemi näol, kuhu andmetöötleja (nt ettevõte, asutus või organisatsioon) koondab ülevaate oma andmetöötlustoimingutest. See sisaldab teavet selle kohta, milliseid isikuandmeid töödeldakse, mis eesmärgil ja kelle poolt.

on artikli 49 lõike 1 teises lõigus osutatud edastamisega, siis sobivate kaitsemeetmete kohta koostatud dokumendid;

- võimaluse korral eri andmeliikide kustutamiseks ette nähtud tähtajad;
- võimaluse korral artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus (nt krüpteerimine, töötajate koolitus, juurdepääsupiirangud dokumentidele ja muudele isikuandmetele, anonümiseerimine).

AKI on pidanud oma juhendmaterjalis[17] oluliseks lisada avaliku sektori asutuste osas isikuandmete töötlemise ülevaatesse ka avaliku teabe režiimi veeru lisamise, st avalik sektori asutus peab näitama andmeliikide kaupa, milline on nende juurdepääsetavus: kas a) juurdepääsupiiranguga teave, b) teabenõudega küsitav teave, c) võrgulehel avaldatav teave või d) avaandmed.

[17] Andmekaitse Inspektsiooni „Isikuandmete töötlejate üldjuhend“.