Töö nimetus:	**Isikuandmete kaitse korralduse ülevaade**		
Töö eesmärk:	Selgitada, kuidas on Kliimaministeeriumi (KliM) valitsemisalas korraldatud isikuandmete töötlemine. Ülevaade koostati koostöös valitsemisala asutuste andmekaitsespetsialistidega (AKS) ning sellega toetatakse isikuandmete töötlemise korralduse läbipaistvust, tõstetakse teadlikkust isikuandmete kaitse nõuetest, ennetatakse võimalikke mittevastavusi ning vajaduse korral aidatakse viia töötlemispraktikad nõuetega kooskõlla. Samuti valideeritakse isikuandmete töötlemisülevaate koostamise senist protsessi.		
Töö läbiviija:	Bernd Rannamägi, siseaudiitor	**Töö eest vastutav isik:**	Maarja Kilter, SAO juhataja
Töö ulatus:	Ülevaate koostamisel selgitati asutuste tegevusi lähtuvalt isikuandmete kaitse üldmääruse (GDPR) nõuetest, sh artiklitest 24 (vastutava töötleja kohustused), 30 (töötlemisülevaade) ja 35 (mõjuhinnangud) ning isikuandmete kaitse seadusest (IKS). Ülevaade hõlmab järgmisi teemasid: välisveebilehe andmekaitsetingimused, koolitused, intsidendihaldus, andmekaitsealased mõjuhinnangud (DPIA), lepingud volitatud töötlejatega, töötlemisülevaate haldamine, sh andmete säilitamise põhimõtted. Ülevaate koostamisel koguti asutustelt info kehtivate protsesside, vastutajate ja praktika kohta ning selgitati koostöökohti ministeeriumi AKSiga isikuandmete töötlemisülevaate koostamisel ja täiendamisel.		
Töö ulatuse piirang:	Töö iseloomust tulenevalt kirjeldati isikuandmete kaitse korralduse olukorda, koondati asjakohased faktid ja tuvastati võimalikud kitsaskohad, mille kohta tehti soovitusi. Käsitletud teemade piires toodi välja ka juhtumid, kus kogutud teabe põhjal ei olnud täidetud selge õigusaktist tulenev korralduslik kohustus. Töö eesmärk ei olnud siiski anda terviklikku hinnangut asutuste kõigi isikuandmete töötlemise toimingute nõuetele vastavusele.		
Lõpparuanne edastatakse:	Hr Kuldar Leis, taristuminister; Hr Erkki Keldo, energeetika- ja keskkonnaminister; Hr Marten Kokk, Kliimaministeeriumi kantsler; Hr Rainer Vakra, Keskkonnaameti peadirektor; Hr Priit Sauk, Transpordiameti peadirektor; Pr Sirli Sipp Kulli, Eesti Geoloogiateenistuse direktor; Pr Egle Hecht , Eesti Loodusmuuseumi direktori kohusetäitja; Hr Taimar Ala, Keskkonnaagentuuri direktor; Hr Andres Laasma, Riigilaevastiku direktor; Hr Marko Arula, Keskkonnaministeeriumi Infotehnoloogiakeskuse direktor.		

24.05.2016 jõustus isikuandmete kaitse üldmäärus (General Data Protection Regulation, GDPR), mis on otsekohalduv õigusakt ning mida hakati kohaldama alates 25.05.2018 pärast kaheaastast üleminekuaega. Eesti võttis GDPRi rakendamiseks vastu isikuandmete kaitse seaduse, mis täpsustab ja täiendab üldmääruse riigis kohaldamist. GDPRi läbiv eesmärk on tugevdada andmetöötlejate ehk vastutavate ja volitatud töötlejate vastutustundlikkust ning ühtlustada andmekaitse reegleid kõigis ELi liikmesriikides. Vastutustundlikkuse põhimõte tähendab, et andmetöötlejad peavad mõistma **andmetöötluse ahelat, omama sellest täielikku ülevaadet ning tagama isikuandmete töötlemise seaduslikkuse, proportsionaalsuse ja läbipaistvuse**.

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

Isikuandmete kaitse õigusraamistik on viimastel aastatel muutunud keerukamaks. Kiire infotehnoloogiline areng on toonud kaasa uusi võimalusi ja riske ning suurendanud vajadust andmekaitsealase kompetentsi järele, et tagada vastavus kehtivatele nõuetele ja vältida rikkumisi. Avaliku sektori asutustel lasub kohustus tagada, et isikuandmete töötlemine on seaduslik, õiglane ja läbipaistev, lähtudes mh eesmärgipärasuse[1] ja minimaalsuse[2] põhimõtetest. Samuti tuleb rakendada piisavaid turvameetmeid, et vältida volitamata juurdepääsu andmetele, sh isikuandmetele. Isikuandmete töötlemisel peab alati olema õiguslik alus, selle puudumisel rikutakse GDPRi artikli 5 lõike 1 punktis a sätestatud seaduslikkuse põhimõtet.

Andmesubjekti õiguste parema tagamise ja läbipaistvuse suurendamiseks on riigi tasandil kavandatud ja ellu viidud mitmeid tegevusi: nt on Justiits- ja Digiministeerium kaalunud avaliku teabe seaduse muutmist viisil, mis muudaks andmejälgija kasutamise avalikus sektoris kohustuslikuks, samuti ajakohastatakse mitmete andmekogude põhimäärusi ning viimasel ajal on avalikus arutelus olnud ka kaamerate kasutamise ja sellega seotud isikuandmete töötlemise küsimused.

[1] **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.

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

Käesolev töö viidi läbi KliM SAO tööplaani kohaselt ning selle teostamisel juhindusid audiitorid siseaudiitori kutsetegevuse raampõhimõtetest ja siseauditeerimise standarditest. Vaadeldav periood oli 01.07.2023–31.12.2025, kuid aruandes on kajastatud ka töö läbiviimise ajal toimunud muudatusi ja asutuste võetud meetmeid, kui need mõjutasid aruande koostamise ajal kehtinud olukorda või järelduste ajakohasust. Ülevaate koostamisel tuginesid audiitorid neile kättesaadavale dokumentatsioonile, töö käigus asutuste esitatud informatsioonile ja selgitustele. Täiendava, audiitoritele mitteesitatud / mitteteadaoleva informatsiooni korral oleksid audiitorite järeldused võinud olla teistsugused.

Täname valitsemisala asutuste andmekaitsespetsialiste meeldiva koostöö eest.

Bernd Rannamägi
Maarja Kilter
/*allkirjastatud digitaalselt*/

TÖÖ TULEMUSTE KOKKUVÕTE

Töö tulemusena anname ülevaate isikuandmete kaitse korralduse hetkeseisust KliM valitsemisalas ning toome välja olulisemad järeldused ja parendusettepanekud.

Positiivsena toome välja, et isikuandmete kaitse korralduses **on mitmes asutuses käesoleva töö ajal toimunud märgatav edasiminek**. Asutused on koostamas või ajakohastamas isikuandmete kaitse kordasid, täiendamas töötlemistoimingute ülevaateid, korrastamas AKSi rolli ja kontaktandmeid ning uuendamas andmesubjektidele avaldatavat teavet. Mitmed töö käigus tuvastatud konkreetsed puudused kõrvaldati juba ülevaate koostamise ajal. Kuigi kavandatud tegevused ei ole kõigis asutustes veel lõpule viidud, näitavad tehtud ja kavandatud sammud, et isikuandmete kaitse korraldus liigub süsteemsema, selgema ja paremini dokumenteeritud töökorralduse suunas.

Samas on isikuandmete kaitse korraldus KliM valitsemisala asutustes jätkuvalt ebaühtlane: asutuste lõikes erinevad nii põhimõtete, rollide ja vastutuse määratletus kui ka nõutavate dokumentide ja töökorralduslike lahenduste olemasolu, ajakohasus ning rakendamise süsteemsus.

Ulatuslikumad korrastamisvajadused ilmnesid ELMis ja EGTs. ELMis ei olnud töö läbiviimise ajal AKSi ülesannete täitmine selgelt korraldatud ega isikuandmete töötlemistoimingute ülevaadet koostatud. Samuti ei olnud ELMi välisveebilt leitav andmesubjektidele mõeldud selgelt eristatav kontaktkanal isikuandmete töötlemise küsimustes. EGTs määrati AKS töö ajal (registriandmed ajakohastati 14.10.2026) ja välisveebis on avaldatud kontaktkanal, kuid välisveebis ei ole avaldatud andmesubjektidele suunatud isikuandmete töötlemise põhimõtteid ning varasema AKSi koostatud esialgne materjal vajab edasiarendamist, et kujundada sellest GDPRi artikli 30 nõuetele vastav töötlemistoimingute register.

Muud parendusvajadused seonduvad eelkõige isikuandmete kaitse põhimõtete ja juhiste kättesaadavuse, AKSi rolli ja kaasamise korralduse ning töötlemisülevaadete ja andmesubjektidele avaldatava teabe ajakohasuse ja täielikkusega. Samuti vajavad tähelepanu koolitus- ja teadlikkuse suurendamise tegevuse süsteemsus ning isikuandmetega seotud rikkumiste, mõjuhinnangute ja volitatud töötlejatega seotud küsimuste dokumenteeritud käsitlemine.

Nende teemade läbimõeldud täpsustamine ja vajaduse korral korrastamine aitaks ühtlustada valitsemisala isikuandmete kaitse praktikat, vähendada protsesside ebaselgust ning tugevdada asutuste suutlikkust tõendada GDPRi vastutustundlikkuse põhimõtte täitmist. Asutustel tuleks jätkata töö käigus tuvastatud puuduste ja parendusvajaduste lahendamist ning viia lõpule juba alustatud või kavandatud tegevused. Kui töö käigus ilmnes õigusaktist tuleneva selge kohustuse täitmata jätmine, tuleb asutusel kavandada tegevused nõuetekohase olukorra saavutamiseks. Muude tuvastatud parendusvajaduste puhul saab asutus valida oma töökorraldusele ja riskidele sobiva lahenduse, mis kõrvaldab või piisavalt maandab järelduses kirjeldatud kitsaskoha. Ettepanekute rakendamise ulatus ja lahendus peavad olema proportsionaalsed asutuse ülesannete, isikuandmete töötlemise laadi ja mahu ning töötlemisega kaasnevate riskidega. Väiksema mahu ja riskitasemega töötlemise korral võib piisata lihtsamast töökorralduslikust või dokumenteeritud lahendusest, kui see võimaldab nõuete täitmist ja tehtud valikuid tõendada.

Ettepanekute rakendamisel tuleb arvestada riigi IKT-korralduses toimuvate muudatustega. RIT ühendatakse 1. jaanuariks 2027 RIAga ning KeMITi ülesanded on kavandatud alates 1. veebruarist 2027 jaotada Riigi Digikeskuse, RIA ja KliMi vahel. Seetõttu tuleb RITile ja KeMITile suunatud või nende osalemist eeldavaid ettepanekuid käsitada senise teenusekorralduse ja üleminekuperioodi kontekstis. **KliMil ja teenindatavatel asutustel tuleb ülesannete ja vastutuse täpsustumisel hinnata, millised isikuandmete kaitsega seotud rollid, korrad, protsessid, teabevahetuse põhimõtted, kontaktpunktid ja koostöökokkulepped tuleb uues teenusekorralduses asjaomaste teenuseosutajatega uuesti määrata või täpsustada**.

Töö tulemused on esitatud teemade kaupa. Iga teema juures on esmalt toodud lähtekoht ehk korralduslik ootus, mille alusel olukorda kirjeldati, seejärel peamised järeldused ja ettepanekud. Ettepanekud on esitatud kas kõigile asutustele või konkreetsetele asutustele, kelle puhul vastav parendusvajadus töö käigus ilmnes. Ettepanekute rakendamisel saab iga asutus valida oma töökorraldusele sobiva lahenduse, kui see maandab järeldustes kirjeldatud kitsaskohta ja võimaldab tegevust dokumenteeritult tõendada.

1. Isikuandmete kaitset korraldavad dokumendid ja juhised

Lähtekoht: Asutuses on kehtestatud selged, ajakohased ja teenistujatele hõlpsasti kättesaadavad isikuandmete kaitset käsitlevad korrad, juhised või muud asjakohased dokumendid, mille sisu on arusaadav, kooskõlas kehtivate nõuetega ning toetab isikuandmete kaitse põhimõtete praktilist rakendamist igapäevases töös. Asutus tagab dokumentide regulaarse

ülevaatamise, vajaduse korral ajakohastamise ning nende tutvustamise viisil, mis võimaldab teenistujatel oma ülesannete täitmisel juhiseid teadlikult ja järjepidevalt järgida. Samuti on asutuses kokku lepitud isikuandmete kaitse alaste koolituste ja teadlikkuse suurendamise põhimõtted ning rakendatakse praktikaid, mis tagavad koolituste regulaarsuse, sihtrühmapõhisuse ja osalemise jälgitavuse. Koolituste sisu, maht ja sagedus lähtuvad teenistujate rollidest, vastutusaladest, juurdepääsust isikuandmetele ning isikuandmete töötlemisega seotud riskidest. Vastutustundlikkuse põhimõtte täitmist toetab see, kui asutuses on tagatud nii uute kui ka olemasolevate teenistujate teadlikkuse kujundamine ja ajakohastamine, asutus kogub ning säilitab ülevaadet koolitustel osalemise kohta ning hindab regulaarselt koolitusvajadust, arvestades mh õigusruumi, tööprotsesside, tehnoloogiliste lahenduste ja riskitaseme muutusi. Koolituste korraldamisega ja teadlikkuse tõstmisega on näiteks seotud järgmised GDPRi artiklid:

- GDPR art 5 lg 2 — vastutustundlikkuse põhimõte;
- GDPR art 24 — vastutava töötleja kohustus rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid;
- GDPR art 32 lg 4 — juurdepääsu omavad isikud võivad andmeid töödelda üksnes vastutava töötleja juhiste alusel;
- GDPR art 39 lg 1 punkt b — AKSi ülesanne jälgida nõuete täitmist, sh teadlikkuse suurendamist ja koolitamist;
- rikkumiste kontekstis ka artiklid 33–34.

JÄRELDUS 1 - isikuandmete kaitse korralduse dokumenteeritus, ajakohasus ja tõendatavus. Kõigis KliM valitsemisala asutustes on isikuandmete kaitse põhimõtteid kirjeldatud ja teenistujatele eri keskkondade kaudu kättesaadavaks tehtud, kuid regulatsioonide terviklikkus, ajakohasus, leitavus ja rakendamise süsteemsus erinevad asutuste lõikes.

TRAMis ja KeMITis on kehtestatud eraldi isikuandmete kaitse kord. TRAMis kuni 02.09.2026 kehtinud andmekaitse kord sisaldas vananenud viiteid MKMi kordadele ning mittetöötavaid linke ning vajas ajakohastamist KliM valitsemisalaga ühinemisest tulenevate muudatuste tõttu. Käesoleva töö ajal kehtestati 03.09.2026 TRAMis ajakohastatud isikuandmete töötlemise kord.

Mitmes asutuses on alustatud isikuandmete kaitse korra koostamist, kuid protsess ei ole kõigil juhtudel jõudnud kehtestatud, ajakohase ja praktikas rakendatava dokumendini. KliMis ja KeAs on korra eelnõud koostatud, kuid kehtestamiseni ei ole jõutud. RiLis oli kord kavandatud kehtestada 2026. aasta II kvartali lõpuks ning EGTs 2026. aasta lõpuks, samas tuleb tagada, et tegevused ei jääks üksnes kavatsuse tasemele.

KAURis ja ELMis seni eraldiseisvat korda kehtestatud ei ole, kuid KAUR kaalub asutusesisese korra koostamist, võttes vajaduse ja sobivuse korral arvesse KliMi väljatöötatava regulatsiooni põhimõtteid.

Kuigi GDPR ei nõua ühe konkreetse nimetusega isikuandmete kaitse korra kehtestamist, peab vastutav töötleja rakendama asjakohaseid korralduslikke meetmeid, suutma nõuetele vastavust tõendada ning meetmeid vajaduse korral ajakohastama. Mitmesse dokumenti ja keskkonda jaotatud, ebapiisavalt seostatud või ajakohastamata juhised võivad raskendada nõuete ühetaolist rakendamist ja nende täitmise tõendamist. Seetõttu on põhjendatud terviklike, ajakohaste, hõlpsasti leitavate ning asutuse tegevuse ja riskidega proportsionaalsete isikuandmete kaitse regulatsioonide väljatöötamine ja ajakohastamine. Regulatsioon ei pea sisalduma ühes dokumendis, kuid asjakohased dokumendid peaksid moodustama selge, sidusa ja ajakohase terviku. Dokumenteeritud, ajakohane ja praktikas rakendatav korraldus toetab GDPRi vastutustundlikkuse põhimõtte täitmist ning aitab asutusel vajaduse korral tõendada, kuidas isikuandmete kaitse nõuete järgimine on korraldatud.

JÄRELDUS 2 — isikuandmete kaitse teabe kättesaadavus siseveebides. KliM valitsemisalas on loodud haldusalaülene isikuandmete kaitse alamleht, mis koondab üldised isikuandmete kaitse põhimõtted, juhised (sh süsteemse ülevaate isikuandmete ja eriliigiliste andmete olemusest, töötlemise põhimõtetest ja õiguslikest alustest ning selgitab vastutava ja volitatud töötleja rolli ning andmesubjekti õigusi, alamlehel on kirjeldatud isikuandmete rikkumisest teavitamise protsess), korduma kippuvad küsimused ja lisatud viited AKI juhenditele ja KliMi koolitusmaterjalile. Alamleht toetab ühtset arusaama andmekaitse nõuetest, kuid ligipääs varasemale alamlehele ei ole tagatud kõigile valitsemisala asutustele, sh TRAMile ja RiLile. RiLi juurdepääsu puudumine haldusala ühisele siseveebile on seotud valitsemisala IT-tehnilise korralduse ja kasutatavate arvutitöökohateenustega. KeMITi IT-teenuse omaniku selgituse kohaselt varasemat haldusala siseveebi enam ei arendata, selle alamlehtedel olevaid materjale ei ajakohastata ega lisata uusi materjale. Varasem siseveeb jääb üleminekuperioodil ligipääsetavaks ning kava kohaselt suletakse see pärast kõigi asutuste üleminekut ATK 2.0 arvutitöökoha teenusele, eeldatavasti 2026. aasta lõpuks. Samas selgitati, et uus haldusala siseveebi leht on SharePointis loodud, kuid sellele ei ole veel kasutusõigusi määratud ning lehe sisu ja edasise arendamise kavandamine on alles algamas. Teiste asutuste puhul ligipääs ühisele siseveebile tagatakse, kuid TRAMile tervikuna ei ole seda kavandatud, samas kaalutakse juurdepääsu võimaldamist üksikutele TRAMi kontaktisikutele. Ülevaate koostamise ajal ei olnud selle lahenduse teostatavus ega täpsem korraldus veel selgunud.

Arvestades haldusalaülese siseveebi ümberkorraldust SharePointi keskkonda ja valitsemisala asutuste liikumist RITi arvutitöökohateenusele, tuleb tagada, et vajalik isikuandmete kaitse teave oleks igas asutuses ajakohasel, püsival ja teenistujatele lihtsalt leitaval kujul kättesaadav. Kui haldusalaülene teave ei ole asutusele ligipääsetav või senine teabekanal muutub, peab asutus tagama samaväärse teabe kättesaadavuse oma siseveebis või muus püsivas

sisekanalis. Vastasel juhul suureneb risk, et teenistujad ei leia õigeaegselt tööks vajalikke juhiseid ning asutusel on keerulisem tõendada, et isikuandmete kaitse nõuete täitmiseks vajalik teavitamine ja juhendamine on korraldatud. Ühise teabekanali tehnilise ligipääsu tagamine eeldab seejuures KliMi, asjaomaste IT-teenuse osutajate ja asutuse koostööd; asutuse vastutus on tagada, et kuni ühise lahenduse tekkimiseni oleks vajalik teave töötajatele kättesaadav alternatiivses sisekanalis.

JÄRELDUS 3 — IT-maja korrad. KeMITi koostatud korrad ja juhised mõjutavad isikuandmete kaitse praktilist korraldust KliMis, KeAs, KAURis, EGTs ja ELMis, kuivõrd KeMIT osutab neile asutustele IT-teenuseid ning tema kehtestatud tehnilised ja infoturbealased nõuded on teenindatavatele asutustele kohustuslikud. Need korrad puudutavad ka isikuandmete kaitse seisukohalt olulisi tööprotsesse, sh infovahendite kasutamist, andmete töötlemist, juurdepääse, logihaldust, andmevarundust ja intsidentide käsitlemist. KeMIT on edastanud vastavad korrad asutustele KIRKE kaudu ning asutused on need teinud teenistujatele DHSi kaudu kättesaadavaks, mis loob eeldused nõuetega tutvumiseks. Samas ei taga üksnes dokumentide kättesaadavaks tegemine kindlust, et teenistujad mõistavad nendes sätestatud andmekaitsealaseid nõudeid või oskavad neid igapäevases töös rakendada.

Asutuste AKSe ei ole alati IT-majade isikuandmete kaitse korraldusega seotud kordade väljatöötamisse kaasatud. Samas kui teenindavatele asutustele kohalduvate IT-maja kordade koostamisel või ajakohastamisel ei kaasata asutuste AKSe, esineb risk, et kordades sätestatud nõuded ei ole piisavalt seotud teenindatavate asutuste tööprotsesside, rollide ja vastutustega ning asutustel on keerulisem tagada ja tõendada GDPRi nõuete täitmist.

KeMITi ülesanded on kavandatud jaotada Riigi Digikeskuse, RIA ja KliMi vahel, kuid ülevaate koostamise ajal ei ole ülesannete ja teenuste lõplik jaotus ega töötajate edasine paiknemine veel kindlaks määratud. **Ümberkorralduse käigus tuleb hinnata, millised KeMITi tegevuse lõppemisel kehtivuse kaotavad isikuandmete kaitse korraldusega seotud KeMITi korrad, tuleb asjaomastes valitsemisala asutustes uuesti kehtestada või olemasolevate kordadega asendada** arvestades KeMITi ülesannete ja teenuseosutuse korralduse muutusi.

JÄRELDUS 4 — isikuandmete kaitse koolituste korralduse ebaühtlus. Isikuandmete kaitse alase teadlikkuse tõstmiseks koolituste korraldus ja regulaarsus on valitsemisala asutustes ebaühtlane.

TRAMis on isikuandmete kaitse koolitusi korraldatud järjepidevalt ja erinevatele sihtrühmadele ning koolituste salvestused on teenistujatele järelvaadatavad.

KliMis ja EGTs toimus 25.11.2025 KliM AKSi korraldatud isikuandmete kaitse koolitus ning KliMis on kavandatud 2026. aastaks täiendav infotund. Teenistujate teadlikkuse toetamiseks on KliM asjaajamise alamlehel kättesaadavad ka strateegiaosakonna nõuniku koostatud nö minikoolitused „Andmekaitse teadlikkuse test“ ja „Märgukirja ja selgitustaotluse test“ ning AKSi koostatud „Isikuandmete kaitse test“.

KeAs toetatakse andmekaitseteadlikkust uute teenistujate sisseelamisõppe, siseveebis kättesaadavate õppematerjalide ja vajaduspõhise nõustamise kaudu ning asutuse teabehalduse alamlehel on kättesaadavad ka KliM strateegiaosakonna nõuniku ja AKSi koostatud eelpool viidatud minikoolitused. Hindamisperioodil ei olnud KeAs siiski välja kujunenud kõiki olemasolevaid teenistujaid hõlmavat järjepidevat ning rolli- ja riskipõhiselt kavandatud asutusesisest koolituskorraldust.

KAURis toimus 09.10.2026 välise koolitaja poolt korraldatud isikuandmete kaitsealane koolitus, mida teenistujal on võimalik järele kuulata ning mille materjalid on leitavad asutuse isikuandmete kaitse teemalehel.

RiLis ei olnud hindamisperioodil süsteemseid asutusesiseseid isikuandmete kaitse koolitusi toimunud, kuid töötajate teadlikkust on toetatud jooksva nõustamise ning välistel koolitustel ja seminaridel osalemise kaudu ning asutuse selgituse kohaselt korraldatakse 2026. aasta novembris ja detsembris kõigile töötajatele organisatsioonisisene koolitus. KeMITis on isikuandmete kaitse koolitus kavandatud 2026. aastaks, kuid hindamisperioodil ei olnud süsteemseid sisekoolitusi toimunud. ELMis ei olnud hindamisperioodil isikuandmete kaitse teemalisi koolitusi korraldatud.

Selline erinev korraldus võib kaasa tuua olukorra, kus teenistujate isikuandmete töötlemise nõuete alase teadlikkuse järjepidev kujundamine ja ajakohastamine sõltub eelkõige asutusepõhisest praktikast, AKSi algatusest ja üksikute teenistujate koolitusvõimalustest.

JÄRELDUS 5 — individuaalse nõustamise ja süsteemse koolituse vahekord. Mitmes asutuses toetatakse teenistujate teadlikkust isikuandmete kaitse nõuetest peamiselt AKSi või andmekaitse töörühma igapäevase nõustamise, siseveebi materjalide ja vajaduspõhiste selgituste kaudu. RiLis on sellisteks teadlikkuse suurendamise tegevusteks olnud lisaks jooksvale nõustamisele töötajate osalemine välistel koolitustel ja seminaridel. Selline lähenemine on oluline ja aitab lahendada konkreetseid tööalaseid küsimusi, kuid ei asenda regulaarset ja sihtrühmapõhist koolitust. Kui teenistujate teadlikkus sõltub üksnes sellest, kas nad oskavad ise küsimust märgata ja AKSi poole pöörduda, suureneb risk, et osa teenistujaid ei teadvusta oma tööülesannetes isikuandmete töötlemist ega rakenda piisavalt GDPRi põhimõtteid, sh seaduslikkuse, minimaalsuse, läbipaistvuse ja turvalisuse nõudeid.

JÄRELDUS 6 — sihtrühmapõhise koolitusvajaduse määramine. Koolitusvajaduse tuvastamine toimub asutustes üldjuhul arenguvestluste, juhtide sisendi, AKSi tähelepanekute või konkreetsete tööprotsesside vajaduse kaudu, kuid isikuandmete kaitse alane koolitusvajadus ei ole kõigis asutustes määratletud süsteemselt ametikohtade, töötlemistoimingute või riskitaseme alusel. Samas näitavad TRAMi, KAURi, RiLi ja KeMITi tähelepanekud, et teadlikkuse vajadus erineb töötajagruppide lõikes: suurem koolitusvajadus võib olla teenistujatel, kes töötlevad isikuandmeid igapäevaselt, süsteemiadministraatoritel, personalitöötajatel, teenuse- ja protsessiomanikel, arenduste tellijatel, projektijuhtidel ning vahetustega või hajusa töökorraldusega teenistujatel. Kui koolitusvajadust ei kaardistata rolli- ja riskipõhiselt, võib koolitus jääda liiga üldiseks ega pruugi toetada nende töötajate praktilist valmisolekut, kelle tööülesannetes andmekaitseriskid kõige enam avalduvad.

JÄRELDUS 7 — isikuandmete kaitse alase teadlikkuse suurendamise tegevuste jälgitavus ja teadmiste ajakohastamine. Kirjeldatud andmete põhjal on mitmes asutuses olemas ülevaade üksikutel koolitustel osalenutest, kuid kogutud teabe põhjal ei ole mitmes asutuses kujunenud süsteemset ja proportsionaalset ülevaadet sellest, millistele teenistujate sihtrühmadele on konkreetne isikuandmete kaitse alane koolitus või muu teadlikkuse suurendamise tegevus suunatud, kas asjakohased sihtrühmad on tegevuses osalenud ning millal tuleb nende teadmisi ajakohastada. RiLis on kavandatud koolituse salvestamine ja teadmiste kontroll, mis toetaks nii koolitusel osalemise jälgitavust kui ka teadmiste kinnistamist, ning KliMis, TRAMis, KeAs, KAURis ja EGTs on koolituste salvestused või materjalid vähemalt osaliselt kättesaadavad järelvaatamiseks. Kui asutusel puudub mõistlik ja proportsionaalne ülevaade teadlikkuse suurendamise tegevuste sihtrühmadest, nende läbiviimisest või kättesaadavaks tegemisest ning teadmiste ajakohastamise vajadusest, on asutusel keerulisem hinnata tegevuste piisavust ja tõendada, et teenistujate isikuandmete kaitse alase teadlikkuse suurendamine on korraldatud järjepidevalt ning lähtub nende rollidest, tööülesannetest ja isikuandmete töötlemisega seotud riskidest.

JÄRELDUS 8 — infoturbe- ja isikuandmete kaitse koolituste omavaheline seos. KliM valitsemisalas on korraldatud infoturbekoolitusi ning mitmes asutuses käsitletakse andmete ja infovahendite kaitset sisseelamis- või infoturbekoolituste raames. Infoturve ja isikuandmete kaitse on omavahel tihedalt seotud ning nende käsitlused kattuvad eelkõige isikuandmete töötlemise turvalisust puudutavates küsimustes, nagu juurdepääsude ja logide haldamine, andmete konfidentsiaalsuse, tervikluse ja käideldavuse tagamine ning turvaintsidentidele reageerimine. Infoturbekoolitused ei pruugi siiski piisavas ulatuses käsitleda isikuandmete töötlemise muid õiguslikke, korralduslikke ja praktilisi aspekte, sh töötlemise õiguslikke aluseid, võimalikult väheste andmete kogumise põhimõtet, andmesubjekti õigusi, töötlemistoimingute dokumenteerimist, andmekaitsealase mõjuhinnangu tegemist ning isikuandmetega seotud rikkumistest teavitamist. Infoturbekoolitust ei saa seega üldjuhul käsitada isikuandmete kaitse koolituse täieliku asendajana, kuid koolituste sisu tuleks kavandada terviklikult, arvestades valdkondade omavahelist seotust ja osalist kattuvust, ning tagada töötajatele nende tööülesannetest lähtuvad vajalikud teadmised nii isikuandmete töötlemise turvalisuse kui ka muude andmekaitsenõuete kohta.

JÄRELDUS 9 — praktikandid ja lepingud. Asutustes on praktikantide lepingutes või praktika kokkulepetes sätestatud konfidentsiaalsusnõuded, mis toetavad isikuandmete ja muu piiratud juurdepääsuga teabe kaitset.

ETTEPANEK KeMITi või RITi teenuseid kasutavatele asutustele:

1. Hinnata KeMITi ümberkorraldamisel ja RITi RIAga ühendamisel, millised senistes IT-teenuse osutaja kordades ja juhistes sätestatud isikuandmete kaitsega seotud põhimõtted jäävad kohaldatavaks ning millised tuleb kajastada asutuse enda dokumentides või uue teenusekorralduse kokkulepetes.

ETTEPANEKUD kõikidele asutustele:

2. Korraldada isikuandmete kaitse korraldust puudutavate kordade, juhiste ja tööprotsesside koostamine või ajakohastamine nii, et asutuse AKS kaasatakse piisavalt varases etapis. See puudutab ka teabehalduse, dokumendihalduse, infoturbe, intsidendihalduse, lepingute ja töökorralduse dokumente, kui need sisaldavad isikuandmete töötlemise, säilitamise, juurdepääsu või rikkumistest teavitamise põhimõtteid. Varane kaasamine aitab tagada, et isikuandmete kaitse nõudeid arvestatakse tööprotsessides enne dokumentide kehtestamist või protsesside kasutuselevõttu. AKSi kaasamise viis võib sõltuda asutuse töökorraldusest, nt võib kaasamine olla korraldatud menetlusse kaasatud teise juristi kaudu, kui on kokku lepitud, et see jurist suunab isikuandmete kaitse korraldust puudutava dokumendi piisavalt varases etapis AKSile ülevaatamiseks või konsulteerib AKSiga (nt KAURis). Oluline on, et valitud töökorraldus tagaks isikuandmete kaitse küsimuste õigeaegse tuvastamise ja AKSi kaasamise enne dokumendi kehtestamist või asjakohase otsuse tegemist.
3. Tagada, et isikuandmete kaitsega seotud korrad, juhised ja muu asjakohane andmekaitseteave tehakse teenistujatele sisuliselt arusaadavaks. Üksnes dokumendi DHSis, siseveebis, juhendite keskkonnas või muus sisekanalis avaldamine ei pruugi olla piisav; teenistujatele tuleks selgitada, millised on nende rollid ja kohustused isikuandmete töötlemisel, millal tuleb pöörduda AKSi poole, kuidas tegutseda võimaliku rikkumise korral ning kust tööks vajalik andmekaitseteave leitav on.

4. Määrata isikuandmete kaitse alaste koolituste ja teadlikkuse tõstmise korraldamise põhimõtted selliselt, et oleks selgelt kirjeldatud koolitusvajaduse tuvastamine, sihtrühmad, koolituste sagedus, vastutajad, osalemise jälgimine ja teadmiste uuendamise kord. Vähemalt tuleks tagada, et uued teenistujad ja praktikandid saavad sisseelamisprotsessi käigus esmase ülevaate isikuandmete kaitse põhimõtetest ning olemasolevatele teenistujatele korraldatakse perioodiliselt rolli- ja riskipõhiseid koolitusi, infotunde või muid teadlikkuse tõstmise tegevusi. Koolituste kavandamisel tuleks arvestada teenistujate tööülesandeid, kokkupuudet isikuandmetega, kasutatavaid infosüsteeme ning varasemate rikkumiste, küsimuste või nõustamisvajaduse põhjal ilmnenud vajadusi.

ETTEPANEKUD KliM AKSile koostöös valitsemisala asutuste AKSidega:

5. Leppida kokku minimaalse teenistujatele kättesaadavaks tehtava isikuandmete kaitse teabe soovituslik koosseis ja avaldada see valitsemisalaülesel loodaval siseveebilehel. Kui asutus ei oma sellele siseveebi lehele ligipääsu, tuleks info olemasolu tagada asutuse sisekanalis. Soovituslik teabe koosseis võiks hõlmata vähemalt isikuandmete töötlemise põhimõtteid ja õiguslikke aluseid, andmesubjekti õigusi, isikuandmetega seotud rikkumistest teavitamise korda, AKSi kontaktandmeid, töötlemistoimingute dokumenteerimise nõudeid, praktikantide ja lepingupartnerite konfidentsiaalsusnõudeid ning asutuses kohaldatavaid andmekaitsealaseid kordi ja juhiseid. Teabe täpse koosseisu, avaldamise koha ja viisi otsustab asutus. **Kokkuvõtlikult tuleb igal valitsemisala asutusel tagada, et asutuse tegevust ja töökorraldust arvestav isikuandmete kaitse teave oleks teenistujatele püsivalt ja lihtsalt leitavalt kättesaadav, selle asukoht oleks teenistujatele teada ning määratud oleks teabe ajakohastamise eest vastutaja ja ülevaatamise sagedus.** See aitab tagada, et teenistujatel oleks sõltumata kasutatavast teabekanalist juurdepääs tööks vajalikule ja ajakohasele isikuandmete kaitse teabele.
6. Töötada välja valitsemisalaüleselt kasutatav isikuandmete kaitse baaskoolitus või lühike juhendmaterjal, mida asutused saavad täiendada oma tööprotsessidest ja riskidest lähtuvate näidetega. Baaskoolitus või juhendmaterjal võiks katta vähemalt isikuandmete mõistet ja eriliigilisi isikuandmeid, töötlemise põhimõtteid ja õiguslikke aluseid, andmesubjekti õigusi, töötlemistoimingute dokumenteerimist, andmekaitsealase mõjuhinnangu vajaduse hindamist, isikuandmetega seotud rikkumistest teavitamist ning teenistuja praktilist vastutust. Materjal peaks olema kättesaadav siseveebis või muus püsivas keskkonnas ning kasutatav nii sisseelamisprogrammis kui ka perioodilise teadmiste uuendamise toetamiseks. Baasmaterjali täiendamiseks sihtrühmapõhiselt saaksid asutused kasutada TRAMi kogemust sihtrühmapõhiste koolituste, salvestuste ja teadlikkuse kaardistamise korraldamisel.

ETTEPANEK KeAle, RiLile, KeMITile, EGTle ja ELMile:

7. Viia kavandatud või vajalikud isikuandmete kaitse koolitused ellu konkreetse ajakava alusel ning määrata koolituste sihtrühmad, vastutajad ja osalemise jälgimise viis. Seejuures tuleks:
   - RiLil viia 2026. aasta novembris ja detsembris läbi kavandatud organisatsioonisisene koolitus, rakendada kavandatud teadmiste kontrolli ning kasutada koolituse sisu täpsustamisel võimaluse korral töötlemisülevaate koostamisel ilmnenud praktilisi küsimusi ja koolitusvajadusi;
   - KeMITil ellu viia 2026. aastaks planeeritud praktiline ja rollipõhine koolitus;
   - EGTl ja ELMil määrata esmane koolitusplaan uutele ja olemasolevatele teenistujatele;
   - KeAl lisada isikuandmete kaitse alane koolitus koolitus- ja arendustegevuste juhtrühma regulaarse planeerimise osaks ning määrata, millise sagedusega ja millistele sihtrühmadele andmekaitsealaseid koolitusi või infotunde korraldatakse, samuti võiks andmekaitse töörühm 2026. aastal kavandatud kohvihommiku või muu formaadi kaudu tutvustada teenistujatele oma rolli, isikuandmete töötlemise põhimõtteid, andmesubjekti õigusi ja töötajate kohustusi.

   Koolituste järel tuleks tagada materjalide kättesaadavus ning vajaduse korral koolituse järelvaatamise võimalus.

ETTEPANEK KeMITile (edaspidi Riigi Digikeskusele ja RIAle) koostöös tema teenindatavate asutustega:

8. Leppida IT-maja ja tema teenindatavate asutuste vahel kokku põhimõtted, mille kohaselt kaasatakse teenindatavate asutuste AKSid IT-maja koostatud isikuandmete kaitse korraldusega seotud kordade, juhiste ja teenuseprotsesside koostamisse ja ajakohastamisse piisavalt varases etapis enne nende kehtestamist või olulist muutmist, kui need korrad, juhised või teenuseprotsessid kohalduvad teenindatavatele asutustele või mõjutavad nende tööprotsesse ja isikuandmete töötlemist. Eelkõige on see vajalik isikuandmetega seotud intsidentide käsitlemist reguleerivate kordade puhul. KeMITi ülesannete ümberkorraldusel Riigi Digikeskusesse, RIAsse ja KliMi tuleb KliMil, teenindatavatel asutustel ja asjaomasel IT-teenuse osutajal tagada, et sama AKSide õigeaegse ja sisulise kaasamise vajadus oleks uues teenusekorralduses selgelt kokku lepitud.

ETTEPANEKUD KliMile:

9. Jätkata KliMis alustatud isikuandmete töötlemise korra eelnõu lõpuleviimisega. Toetame KliMi kavandatud lahendust koondada isikuandmete töötlemise põhimõtted, rollid, vastutus ja juhised teenistujatele ühte selgelt kättesaadavasse dokumenti. Enne kasutusele võtmist tuleks eelnõu üle vaadata selliselt, et see oleks teenistujatele praktiliselt kasutatav, ei dubleeriks liigselt üldist õigusraamistikku ning sisaldaks selgeid juhiseid igapäevaseks tööks. Samuti tuleks määrata lõpuleviimise tähtaeg, vastutav isik või roll ning korra edaspidise ülevaatamise ja ajakohastamise põhimõtted.
10. Lisada uute teenistujate infopäeva või sisseelamisprogrammi isikuandmete kaitse lühitutvustus, nagu KliM on kavandanud.

ETTEPANEK TRAMile:

11. Peale seda, kui TRAMile on KliMi poolt võimaldatud juurdepääs valitsemisalaülesele isikuandmete kaitse teabele, soovitame TRAMil tagada oma teenistujatele ligipääs mainitud teabele või teha kättesaadavaks samaväärne teave asutuse enda siseveebis.

ETTEPANEK KeAle:

12. Jätkata KeAs alustatud isikuandmete kaitse korra eelnõu lõpuleviimise ja kooskõlastamisega. Toetame KeA kavandatud lahendust kirjeldada isikuandmete kaitse põhimõtted, rollid, vastutus ja teenistujatele vajalikud juhised asutusepõhises korras. Soovitame määrata protsessi lõpuleviimiseks tähtaeg ja vastutav isik või töörühm ning pärast lahenduse kasutusele võtmist tagada selle sisuline tutvustamine teenistujatele viisil, nagu asutus on eelnõu juures kavandanud.

ETTEPANEK KAURile:

13. Otsustada juhtkonna tasandil, millisel kujul kirjeldatakse KAURi isikuandmete kaitse korraldus edaspidi. Kui KAUR otsustab lähtuda KliMi võimalikest valitsemisalaülestest põhimõtetest, tuleks määrata, kuidas kaetakse KAURi spetsiifilised tööprotsessid, sh seirekaamerate ja muud asutusepõhised andmetöötlused. Kui valitsemisalaülest lahendust ei kehtestata või see ei kata KAURi tööprotsesse piisavalt, kaaluda koostada asutusesisene juhis, kord või muu samaväärne lahendus. Otsuse tegemiseks ja edasiste tegevuste kavandamiseks tuleks määrata tähtaeg ja vastutaja.

ETTEPANEK RiLile:

14. Jätkata RiLis kavandatud isikuandmete kaitse korra koostamisega. Toetame RiLi plaani kirjeldada korras isikuandmete kogumise, kasutamise, säilitamise ja kaitsmise põhimõtted ning andmekaitsealase mõjuhinnangu koostamise korraldus. Soovitame määrata protsessi lõpuleviimiseks ajakohase tähtaja ja vastutaja ning tagada, et valmiv lahendus oleks teenistujatele kättesaadav ja praktiliselt kasutatav.

ETTEPANEK EGTle:

15. Jätkata EGTs AKSi kavandatud isikuandmete kaitse korralduse kirjeldamisega hiljemalt 2026. aasta lõpuks. Toetame plaani koostada eraldiseisev isikuandmete kaitse kord või muu samaväärne juhend, milles koondatakse isikuandmete töötlemise põhimõtted, rollid ja vastutus, andmesubjekti õiguste tagamine, rikkumistest teavitamine ning seosed infoturbe ja teabehalduse juhistega. Kaasata AKS asutuse SharePointi-põhise siseveebi arendamisse, et isikuandmete kaitse materjalid oleksid teenistujatele kättesaadavad ja loogiliselt üles ehitatud.

ETTEPANEK ELMile:

16. Kaaluda ELMis isikuandmete kaitse korra või muu samaväärse juhendi koostamist, et koondada teenistujatele ühte selgelt leitavasse kohta isikuandmete kaitse korralduse põhimõtted ja praktilised juhised. Sellise lahenduse kasutamist toetab asjaolu, et ELMis ei ole eraldi isikuandmete kaitse korraldust koondavat dokumenti ning AKSi rolli, andmekaitseküsimuste kontaktpunkti ja isikuandmetega seotud rikkumisest teavitamise korralduse nähtavus vajab korrastamist. Korras või juhendis tuleks vähemalt kirjeldada isikuandmete töötlemise üldpõhimõtted, teenistujate kohustused, andmekaitseküsimuste kontaktpunkt, isikuandmetega seotud rikkumisest teavitamise põhimõtted ning teabe ajakohastamise eest vastutav isik või roll. Samuti tuleks tagada, et ELMi teenistujatele oleks arusaadav, millised RITi korrad neile kohalduvad, ning et need oleksid kergesti leitavad ja kasutatavad.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*
KliM	Ootame KeMITi ümberkorraldamise ja RITi ning RIA ühinemise ära ja siis alustame kordade hindamise protsessi. Teadlikkuse tõstmise osas korraldame hetkel KliM haldusalaülest andmekaitse baaskoolitust, mis toimub 11. detsembril 2026. Plaanis on ka koostada uutele teenistujatele andmekaitse baaskoolitus ja test, sarnaselt kuidas nt infoturbel. Uurime, milline keskkond selleks

	kõige parem oleks. Töötlemise kord on prioriteetide järjekorras esikohal, lõpuleviimise tähtaeg on 2027. aasta esimese kvartali lõpp (koos kooskõlastustega), vastutav isik on KliMi AKS Marie Frosch.
TRAM	**Kommentaar ettepaneku punktile 2 (AKSi kaasamine tööprotsessidesse):** Oleme nõus, et AKSi kaasamine protsesside varases etapis on vajalik ja oluline, et tagada isikuandmete kaitse nõuete õigeaegne arvestamine. Samas tuleb AKSi kaasamisel lähtuda asutuse tööprotsesside sisust ja eripärast ning tagada tema kaasamine eelkõige juhtudel, kus tegevus hõlmab isikuandmete töötlemist. Selline lähenemine võimaldab tagada andmekaitsenõuete järgimise, vältides samal ajal AKSi põhjendamatut koormamist küsimustega, mis ei kuulu tema pädevusvaldkonda. **Kommentaar ettepaneku punktile 3 (Teenistujate teadlikkuse suurendamine):** Oleme nõus, et isikuandmete kaitsega seotud korrad ja juhised peavad olema teenistujatele sisuliselt arusaadavad. Selle toetamiseks on võimalik korraldada täiendavaid infotunde ja koolitusi ning kasutada teadmiste kinnistamiseks ja kontrollimiseks näiteks kontrollteste. **Kommentaar ettepaneku punktile 4 (Isikuandmete kaitse alane koolitustegevus):** Asutuses toimub süsteemne isikuandmete töötlemise ja kaitse alane koolitustegevus, mille eesmärk on järjepidevalt suurendada teenistujate teadlikkust ja teadmisi. Uute teenistujate ja praktikantide esmaseks juhendamiseks on olemas koolitusslaidid ja video. Lisaks nõustab asutuse AKS teenistujaid igapäevaselt isikuandmete töötlemisega seotud küsimustes Teamsi, e-posti ja telefoni teel. **Kommentaar ettepanek TRAM-ile (ettepaneku punkt 11) (Ligipääs valitsemisalaülesele andmekaitseteabele):** Asutus on valmis tegema valitsemisalaülese isikuandmete töötlemise ja kaitse alase teabe oma teenistujatele kättesaadavaks, kui KliM võimaldab asutusele vastava juurdepääsu. Juurdepääsu saamisel tagame teabe jagamise teenistujatele asutuse töökorraldusele sobival viisil.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	KAUR teeb otsuse isikuandmete kaitse korra vormi osas, st kas hakkab kasutama valitsemisalaülest lahendust või koostab asutusesisese juhise, pärast KliMi poolt kehtestatava korraga tutvumist. Otsus tehakse 30 päeva ja kord kehtestatakse 6 kuu jooksul pärast KliMi korra jõustumist, vastutaja AKS.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest. **Audiitori märkus:** RiLi täpsustuste põhjal on aruande vastavaid käsitlusi täiendatud.
KeMIT	Nõus ettepanekuga, kuid hea oleks täpsemalt aru saada, milliste kordade loomises soovivad AKS-id kaasa lüüa. Väga paljud korrad on tegelikult KeMIT-i sisesed korrad, kuid tegelikult võib-olla peaksid olema valitsemisala ülese korrad ehk ministeeriumi poolt kinnitatud (KeMIT-i sisene kord ei ole kohustuslik valitsemisala asutustele).
EGT	EGT peab ettepanekuid asjakohaseks. Toetame ühise baaskoolituse või juhendmaterjali koostamist, mida asutused saavad oma tööprotsesside näidetega täiendada. Koolituste ühendamine infoturbe teemadega on sobiv, kui vajalikud andmekaitseteemad on sisuliselt kaetud.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud.

	AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

2. Andmekaitsespetsialisti roll

Lähtekoht: Asutus on määranud AKSi ning korraldanud tema rolli täitmise viisil, mis toetab GDPRi artiklitest 37–39 tulenevate nõuete täitmist, sh taganud AKSi sõltumatuse ja piisavate ressursside ning pädevuste olemasolu. AKS nõustab asutust ja teenistujaid, jälgib isikuandmete kaitse nõuete täitmist ning on kaasatud mõjuhinnangute koostamisse. Asutus on taganud, et oleks korraldatud kontaktpunkti funktsioon andmesubjektide ja Andmekaitse Inspektsiooniga suhtlemisel.

JÄRELDUS 10 — AKSi määramine, registriandmete ajakohasus ja kontaktpunkti nähtavus. KliM valitsemisala asutustes on AKSi määramise kohustus üldjuhul täidetud: KliMis, TRAMis, KeAs, KAURis, RiLis ja KeMITis on AKSi rolli täitja määratud ning kontaktandmed e-äriregistris avaldatud. Samas ilmnes mitmes asutuses, et AKSi andmeid ei olnud e-äriregistris ajakohastatud õigeaegselt või viidi registriandmed tegeliku rollitäitjaga vastavusse alles oluliselt hiljem pärast rollimuutust. **EGTs on AKSi rolli täitja määratud ja asutus on võimaldanud talle erialast täiendkoolitust. E-äriregistri 01.09.2026 andmete kohaselt oli AKSina jätkuvalt märgitud varasem rollitäitja. Aruande kommenteerimise ajal ajakohastati registriandmed ning alates 14.10.2026 on EGTs AKSina registris märgitud tegelik rollitäitja. ELMis ei olnud töö ajal AKSi andmed e-äriregistris ajakohased ning registris oli AKSina märgitud isik, kelle teenistussuhe oli lõppenud 19.01.2022**. Töö käigus esitatud teabe põhjal ei ole ELMis AKSi ülesannete täitmine selgelt korraldatud ning vajab juhtimistasandil otsustamist ja rolli määratlemist. **Samuti ei olnud ELMi välisveebilt leitav selgelt eristatav kontaktkanal andmekaitseküsimuste esitamiseks.**
GDPRi artikli 37 lõike 7 kohaselt peab vastutav või volitatud töötleja avaldama AKSi kontaktandmed ja teavitama neist järelevalveasutust. Ajakohastamata e-äriregistri andmed, ebaselgelt vormistatud roll või avalikult leitava kontaktpunkti puudumine vähendavad AKSi rolli nähtavust ning takistavad andmesubjektidel ja Andmekaitse Inspektsioonil asutuse andmekaitseküsimuste kontaktpunktiga ühendust võtta. Ka on asutusel sellisel juhul keerulisem tõendada GDPRi artikli 37 lõikes 7 sätestatud kontaktandmete avaldamise ja järelevalveasutuse teavitamise kohustuse täitmist.
JÄRELDUS 11 — AKSi aruandlusliin ja sõltumatus. AKSi sõltumatuse tagamiseks peab asutuse aruandluskorraldus võimaldama tal täita GDPRi artiklites 38–39 sätestatud ülesandeid sõltumatult ning anda aru otse asutuse kõrgeimale juhtimistasandile. See ei eelda tingimata AKSi organisatsioonilist otsealluvust asutuse juhile, vaid selgelt määratletud sõltumatut aruandlusliini, vahetut juurdepääsu kõrgeimale juhtimistasandile ja võimalust esitada oma seisukohti ilma juhisteta. KeAs ja KeMITis toetab sõltumatut aruandlust korraldus, mille kohaselt tegutseb AKS või andmekaitse töörühm direktori või peadirektori otsealluvuses. KliMis on kavandatud või alustatud muudatusi, mille eesmärk on korraldada AKSi aruandlus vahetult kantslerile või asutuse juhile (nt KliM AKSi ametijuhendis, veel kehtestamata, on sõnastatud aruandlusliin kantslerile). EGTs allub AKSi ülesandeid täitev isik õigusnõunik juba vahetult direktorile; AKSi sõltumatu aruandluse põhimõtted tuleb vajaduse korral töökorralduslikes dokumentides täpsustada. TRAMis, KAURis ja RiLis paikneb AKSi ametikoht formaalselt keskastmejuhi alluvuses, kuid kogutud teabe kohaselt on AKSile tagatud sõltumatu aruandlusliin ja võimalus pöörduda kõrgeima juhtimistasandi poole. ELMis vajab AKSi roll, aruandlusliin ja juurdepääs kõrgeimale juhtimistasandile täpsustamist. Kui sõltumatu aruandlusliin, vahetu juurdepääs kõrgeimalejuhtimistasandile ja võimalus esitada oma seisukohti ei ole selgelt korraldatud ega dokumenteeritud, suureneb risk, et AKSi sõltumatus ja GDPRi artikli 38 lõike 3 nõuete täitmine ei ole piisavalt tagatud ega tõendatav.
JÄRELDUS 12 — ressursid. Kogutud teave näitab, et valitsemisala asutustes, kus AKSi roll on määratud, on AKSidele üldjuhul tagatud ametijuhendis, töökorralduslikus kokkuleppes või andmekaitse töörühma moodustamise otsuses sätestatud ülesannete täitmiseks vajalikud töövahendid, tehnilised ressursid ja ligipääsud. See loob eeldused AKSi funktsiooni toimimiseks ning toetab GDPRi artikli 38 lõike 2 nõude täitmist, mille kohaselt peab vastutav töötleja toetama AKSi tema ülesannete täitmisel, tagades selleks vajalikud ressursid, sh juurdepääsu isikuandmetele ja töötlemistoimingutega seotud teabele. Samas ei piirdu AKSi ülesannete täitmiseks vajalik ressurss üksnes tehniliste vahendite ja ligipääsudega. GDPRi artikli 38 nõuete täitmiseks peab asutus tagama ka AKSi piisava kaasamise, sõltumatuse, võimaluse täita ülesandeid ilma huvide konfliktita ning realistliku tööaja andmekaitsega seotud ülesannete täitmiseks.
JÄRELDUS 13 — AKSi töömaht ja ülesannete ühildatavus. Kogutud teabe põhjal on mitmes valitsemisala asutuses AKSi rolli täitmise oluliseks väljakutseks ajapuudus ja töömahu kasv. Enamikus valitsemisala

asutustes täidetakse AKSi rolli põhiülesannete kõrval: KAURis, RiLis, KeMITis ja EGTs osalise töömahuga või vajaduspõhiselt, KeAs andmekaitse töörühmana põhiülesannete kõrval ning ELMis täidetakse AKSi ülesandeid lisaülesandena, kuid rolli formaalne korraldus vajab täpsustamist. RiLi selgituse kohaselt mõjutas AKSi töökoormust ülevaateperioodil tavapärasest enam töötlemistoimingute ülevaate koostamine ja käesoleva töö läbiviimises osalemine. Seetõttu ei pruugi töö läbiviimise ajal kirjeldatud koormus kajastada tavapärast töömahtu pärast nende ajutise iseloomuga tegevuste lõppemist. TRAMis täidetakse AKSi ülesandeid täiskoormusega. KliMis on AKSi ülesannete täitmine struktuurimuudatuse järgselt seatud prioriteediks, et viia lõpule GDPRist tulenevate vastutava töötleja kohustuste täitmiseks vajalikud korralduslikud meetmed, sh isikuandmete kaitse korra ja isikuandmete töötlemise ülevaate koostamine. Selleks on ajutiselt vähendatud AKSi rolli täitva isiku muid auditialaseid ülesandeid. Mitmes asutuses ei ole AKSi ülesannete täitmiseks vajalikku töömahtu eraldi määratletud ega regulaarselt hinnatud. Kui tegelik töömaht ületab AKSi ülesannete täitmiseks eraldatud aja või nende täitmine sõltub teenistuja võimalustest põhiülesannete kõrval, suureneb risk, et GDPRi artiklis 39 sätestatud ülesandeid ei täideta nõuetekohaselt ja järjepidevalt. Samas AKSi ülesannete täitmine lisaülesandena ei ole GDPRiga vastuolus, kuid asutus peab artikli 38 lõike 2 kohaselt tagama AKSile ülesannete täitmiseks vajalikud vahendid, sh piisava aja, ning artikli 38 lõike 6 kohaselt vältima huvide konflikti. Huvide konflikt võib tekkida eelkõige juhul, kui AKSil on muu rolli raames pädevus määrata isikuandmete töötlemise eesmärke või vahendeid ning ta peaks AKSina hindama või kontrollima enda tehtud otsuseid. AKSi töömahu regulaarne hindamine, ülesannete ja vastutuse selge piiritlemine ning nende täitmiseks vajaliku aja määramine aitaksid tagada AKSi ülesannete tulemusliku, järjepideva ja sõltumatu täitmise.

JÄRELDUS 14 — AKSi ülesannete järjepidevus ja asendamine. AKSi ülesannete täitmise järjepidevuse tagamiseks on asutustes kasutusel erinevad lahendused, kuid kõigis asutustes ei ole AKSi eemaloleku ajaks määratud vastutus ja kontaktpunkti toimimine piisavalt selgelt kirjeldatud. TRAMis ja RiLis on rakendatud asendamist või kontaktpunkti järjepidevat toimimist toetavad lahendused ning KeAs toetab ülesannete järjepidevust töörühmapõhine töökorraldus. KliMis ja KeMITis vajab täpsustamist andmekaitse postkasti jälgimise ning saabunud pöördumiste menetlemise korraldus AKSi eemaloleku ajal. AKSide selgituste kohaselt jälgivad nad postkasti ka puhkuse ajal. Selline praktika aitab küll tagada pöördumiste märkamise, kuid ei ole jätkusuutlik asendamise korraldus, kuna ülesannete täitmine sõltub ühe teenistuja kättesaadavusest ka tema töölt eemaloleku ajal. KliMis muutus töö läbiviimise ajal AKSi rolli täitja ning andmekaitse postkastile on ligipääs ka siseauditi osakonna juhatajal. Samas ei taga üksnes postkastile ligipääsu olemasolu ülesannete järjepidevat täitmist, kui selgelt ei ole määratud vastutust saabunud pöördumiste menetlemise ja neile õigeaegse vastamise eest. EGTs on asendamine kokkuleppeliselt korraldatud üldosakonna juhataja kaudu, kuid AKSi rolli ja asendamise korralduse formaalne kirjeldamine vajab lõpuleviimist. KAURis vajavad täpsustamist AKSi asendamise ning talle suunatud andmekaitsealaste pöördumiste järjepideva menetlemise põhimõtted tema äraoleku ajal. ELMis vajavad AKSi asendamise ning kontaktpunkti toimimise põhimõtted täpsustamist. Kui AKSi asendamise kord, vastutus ja kontaktpunkti toimimine ei ole selgelt määratud ega dokumenteeritud, suureneb risk, et andmesubjektide pöördumised, isikuandmetega seotud rikkumisteated või järelevalveasutuse päringud ei saa AKSi eemaloleku ajal õigeaegset tähelepanu ega nõuetekohast menetlust. Seetõttu on oluline määrata asutustes AKSi eemaloleku ajaks pädev asendaja või muu toimiv töökorraldus ning sätestada selgelt postkasti jälgimise, pöördumiste menetlemise ja vajaduse korral eskaleerimise vastutus.

JÄRELDUS 15 — AKSide koostöö ja KliM AKSi koordineeriv roll. Valitsemisala AKSide vahel on loodud esmased koostöökanalid, sh Teamsi kanal ja e-posti list ning 24.09.2029 toimus ka esimene valitsemisala AKSide ühine kohtumine, kus lepiti kokku, et regulaarseid ühisarutelusid korraldatakse vähemalt kord kahe kuu jooksul. AKSide intervjuudes kirjeldatud ootused puudutavad eelkõige KliM AKSi rolli selgemat määratlemist koostöö koordineerimisel, metoodilise toe pakkumist, mõjuhinnangute ja andmejälgija rakendamise küsimustes juhendamist, koolitusmaterjalide jagamist ning keerukamate juhtumite põhjal ühisõppe võimaldamist. Kuna iga asutus vastutab oma andmekaitse korralduse eest ise, ei peaks KliM AKS võtma üle asutuste AKSide ülesandeid, kuid selgem koostöö- ja infovahetuskorraldus aitaks toetada GDPRi nõuete põhjendatud ja dokumenteeritud täitmist valitsemisala asutustes.

JÄRELDUS 16 — AKSi varajane kaasamine ja rollide selgus. Mitmes asutuses ilmnes vajadus täpsustada AKSi õigeaegse kaasamise põhimõtteid ning eri osapoolte rolle ja vastutust isikuandmete töötlemisega seotud küsimuste lahendamisel. AKS tuleb nõuetekohaselt ja õigeaegselt kaasata kõigisse isikuandmete kaitset puudutavatesse küsimustesse, sh infosüsteemide arendustesse, andmekaitsealaste mõjuhinnangute tegemisse, hangete ja lepingute ettevalmistamisse, õigusloomesse, uute teenuste kavandamisse, andmete jagamise korraldamisse ning säilitustähtaegade ja juurdepääsupiirangute määramisega seotud otsustesse. Samuti peab AKS olema vajaduse korral kaasatud teabenõuete lahendamisse.

Näiteks TRAMis saab AKS andmekaitsealase mõjuhinnangu tegemise vajadusest sageli teada alles arenduse hilisemas etapis või pärast infosüsteemi kasutuselevõttu. KeA isikuandmete kaitse korra eelnõus on kirjeldatud

töörühma ühine roll, üldkontakti haldamine ning juhtumivastutaja määramine keerukamate kaasuste korral. Praktikas lepitakse töörühma ülesannete jaotus kokku juhtumipõhiselt, lähtudes liikmete pädevusest ja konkreetse küsimuse sisust. Töörühma liikmete vastutusvaldkonnad ja tööjaotus ei ole siiski dokumenteeritult fikseeritud. Samuti ei teadvusta protsessi- ja teenuseomanikud alati piisavalt oma esmast vastutust isikuandmete töötlemise õiguspärasuse ja nõuetele vastavuse tagamisel.

Kui AKSi kaasamise alused, ajastus ja kord ning protsessi- ja teenuseomanike vastutus ei ole selgelt kindlaks määratud, suureneb risk, et isikuandmete töötlemisega seotud õiguslikke ja korralduslikke riske ei tuvastata ega hinnata enne töötlemise alustamist, teenuse käivitamist või infosüsteemi kasutuselevõttu. Selle tulemusena võib AKSi roll kujuneda ennetava nõustamise asemel valdavalt tagantjärele reageerivaks ning vajalike muudatuste tegemine võib olla keerukam, kulukam või ajamahukam.

ETTEPANEK ELMile:

17. **ELMi direktoril tuleks viivitamata määrata ja vormistada AKSi rolli täitja ning kirjeldada tema ülesanded, vastutus, aruandlusliin, rolli täitmiseks vajalik tööaeg, asendamine ja kontaktpunkti toimimise kord.** AKSi rolli võib korraldada asutuses sobiva tööajamahuga või GDPRi artikli 37 lõike 3 alusel ühise AKSina koostöös teise valitsemisala asutusega. Valitud korraldus tuleb kirjalikult kokku leppida. Samuti tuleb ajakohastada e-äriregistri andmed ning avaldada asutuse veebilehel selgelt leitavad kontaktandmed või pöördumiskanal isikuandmete kaitsega seotud küsimuste esitamiseks.

ETTEPANEK EGTle:

18. Viia lõpule EGTs kavandatud AKSi rolli vormistamine ning kajastada AKSi ülesanded töölepingu lisas või ametijuhendis, määrata rollile realistlik töömaht, aruandlusliin ja asendamise ning kontaktpunkti toimimise kord.

ETTEPANEK TRAMile, KAURile, RiLile ja ELMile:

19. GDPRi artikli 38 lõike 3 ja EDPB „Suunistele andmekaitseametnike kohta“ kohaselt peab AKSil olema sõltumatu juurdepääs organisatsiooni kõrgeimale juhtimistasandile. TRAMil, KAURil ja RiLil tuleks üle vaadata AKSi aruandlusliin ja juhtkonnale juurdepääsu korraldus ning vajaduse korral täiendada ametijuhendit, sisekorda või muud töökorralduslikku dokumenti. Korraldus peab selgelt tagama AKSi võimaluse pöörduda vahetult asutuse kõrgeima juhtimistasandi poole ning esitada sõltumatult oma seisukohad, sh vajaduse korral eriarvamus. ELMil tuleks sama põhimõtet arvestada AKSi rolli ja aruandluskorra määramisel. Selgelt reguleeritud aruandlusliin aitab tagada AKSi sõltumatuse, toetab GDPRi nõuete täitmist ja vähendab huvide konflikti riski.

ETTEPANEK asutustele, kus AKSi roll on lisaülesanne (KliM, KeA, KAUR, RiL, KeMIT, EGT ja ELM):

20. Asutustel tuleks hinnata AKSi rolli täitmiseks vajalikku tegelikku töömahtu ja tagada, et AKSil oleks GDPRi artiklites 38–39 sätestatud ülesannete täitmiseks piisav ja realistlik tööaeg. Kui AKSi rolli täidetakse lisaülesandena, tuleb hinnata, kas põhiülesanded võivad takistada nõustamise, vastavuse jälgimise, teadlikkuse tõstmise, mõjuhinnangute nõustamise ja järelevalveasutusega koostöö ülesannete täitmist. Vajaduse korral tuleks korrigeerida tööülesandeid, jagada ülesandeid ümber, kaasata täiendavaid inimesi viisil, mis välistab huvide konflikti ja tagab andmekaitsefunktsiooni sõltumatuse, või kaaluda eraldi AKSi ametikoha loomist. Hindamisel tuleks eristada püsivaid ülesandeid ajutistest suuremahulistest tegevustest, näiteks töötlemisülevaate esmakordsest koostamisest või ulatuslikust ajakohastamisest.

ETTEPANEK KeAle:

21. Koondada ja vajaduse korral täpsustada andmekaitse töörühma olemasoleva töökorralduse kirjeldust, eelkõige liikmete sisemist tööjaotust ja ülesannete järjepideva täitmise korraldust. Kirjelduses arvestada juba rakendatud peadirektori otsealluvuse ja töörühmapõhise asendamise lahendusega.

ETTEPANEK KliMile:

22. KliMil tuleks koostöös valitsemisala asutustega kokku leppida AKSide regulaarse koostöö ja infovahetuse praktiline korraldus. Kokkulepe peaks määrama vähemalt, milliseid teemasid käsitletakse ühiselt, kui sageli infot vahetatakse, millises kanalis jagatakse juhiseid ja materjale ning milline on KliM AKSi koordineeriv roll. Korralduse eesmärk peaks olema metoodilise toe, ühise õppimise ja kogemuste vahetuse toetamine ning keerukamate juhtumite üldistatud käsitlemine, mitte asutuste AKSide ülesannete ülevõtmine ega täiendava formaalse aruandluskohustuse loomine. Kaaluda tasub infoturbe juhtrühmale sarnase, kuid mahult ja töökorralduselt proportsionaalse andmekaitse koostööformaadi loomist.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*

KliM	AKSi eemaloleku ajaks on mõistlik korraldada AKSi postkasti jälgimine SAO osakonnajuhataja kaudu, kellel on postkastile ligipääs ning kes saab vajadusel pöördumised edasi suunata või kaasata teisi asjakohaseid spetsialiste. Samuti on aruandes nimetatud koostöömeetmete osas juba tehtud mitmeid samme. Tagasiside andmise ajaks on loodud ja kasutusele võetud AKSide ühine Teamsi keskkond ja e-posti list ning alustatud regulaarsete kohtumistega, kus arutatakse valdkonnas tekkinud küsimusi ning jagatakse kogemusi ja häid praktikaid. Kavandatud on ühine koolitus ning KliMi AKS tegeleb täiendavate koostöövormide arendamisega, nagu ühine uudiskiri, juhised ja dokumendipõhjad. AKSi õigeaegse kaasamise toetamiseks on kavas koostada siseveebi praktiline juhis, mis aitaks töötajal hinnata, millistes küsimustes ja millises etapis tuleb AKS kaasata.
TRAM	**Kommentaar ettepanek TRAM-ile** (ettepaneku punkt 19): Asutuses paikneb AKSi ametikoht keskastmejuhi alluvuses, kuid AKSil on võimalus pöörduda vahetult asutuse kõrgeima juhtimistasandi, sealhulgas peadirektori või juhtkonna poole. AKSil on võimalus esitada oma seisukohti sõltumatult ning juhtida juhtkonna tähelepanu andmekaitsega seotud küsimustele ja riskidele. Eeltoodust tulenevalt ei näe asutus praegu vajadust muuta AKSi ametikoha paiknemist organisatsioonilises struktuuris. Samas peame oluliseks, et AKSi vahetu juurdepääs kõrgeimale juhtimistasandile ja võimalus esitada sõltumatult oma seisukohti oleksid selgelt tagatud ka töökorralduslikult, kuid oleme valmis vajaduse korral täpsustama sõltumatu juurdepääsu korraldust.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Aruandluse korraldus reguleeritakse isikuandme kaitse korras, millise tähtajad ja vastutaja on toodud ülal. AKSil on võimalik oma töökoormust eri ülesannete vahel paindlikult juhtida. Täna on KAURis tavapärane, et töötaja täidab mitut rolli ning jagab oma töökoormust erinevate ülesannete vahel. Selline töökorraldus võimaldab tänaste eelarveliste vahendite juures tagada organisatsiooni tõhusa toimimise.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	KLIMi ettepanek info liikumise kohta juba jõustatud auditeerimise ajal.
EGT	Nõustume ettepanekutega.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud. AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

3. Töötlemisülevaated

Lähtekoht: Asutusel peab olema ajakohane isikuandmete töötlemisülevaade (töötlemistoimingute register), mis sisaldab GDPRi artiklis 30 nõutud andmeid, sh vastutava töötleja ja AKSi kontaktandmeid, töötlemise eesmärke, andmesubjektide ja

isikuandmete kategooriaid, vastuvõtjate kategooriaid, andmete edastamist ning võimaluse korral säilitustähtaegu ja turvameetmete üldist kirjeldust. Ülevaate haldamine peab olema selgelt korraldatud, määratud vastutajatega ja kirjeldatud ajakohastamise korraga. Kui ülevaade ei ole veel valminud, peavad olema määratletud selle koostamise etapp, planeeritud halduskorraldus ja vastutajad.

JÄRELDUS 17 — Isikuandmete töötlemistoimingute dokumenteerimise valmidus ja GDPRi artikli 30 nõuete täitmine. KliM valitsemisala asutustes on isikuandmete töötlemistoimingute dokumenteerimise valmidus ebaühtlane. Kuigi GDPR ei nõua töötlemistoimingute registri pidamist kindlas vormis ega ühe koonddokumendina, peab vastutav töötleja pidama kirjalikus, sh elektroonilises vormis registrit GDPRi artikli 30 lõikes 1 nimetatud töötlemistoimingute kohta ning volitatud töötlejana tegutsemise korral artikli 30 lõikes 2 nimetatud töötlemistoimingute kohta ja hoidma registris sisalduva teabe ajakohasena.

TRAMis, KeAs ja KeMITis on töötlemisülevaade koostatud, kuid nende puhul ilmnes vajadus ülevaate sisulise täiendamise ja ajakohastamise järele. KliMis on ülevaade osakondadega läbi vaadatud ligikaudu 75% ulatuses, kusjuures viie osakonna andmed põhinevad veel eelkaardistusel. RiLis on ülevaade koostatud ligikaudu 80% ulatuses. KAURis on info kogumine ja kaardistamine pooleli ning selle lõpuleviimiseks on asutus kaasanud välise teenusepakkuja, kelle ülesanne on 08.09.2026 sõlmitud lepingu kohaselt koostada asutuse isikuandmete töötlemistoimingute ülevaade ja töö aruanne hiljemalt 12.11.2026. EGT varasem AKS koostas esialgse isikuandmete töötlemise ülevaate, edastas selle 31.01.2026 asutuse praegusele AKSile ning kavandas täiendamist vajava ülevaate edasiarendamist 2026. aasta jooksul. **ELMis ei olnud töö läbiviimise ajal isikuandmete töötlemise ülevaadet koostatud ega selle koostamist alustatud.**

Töö läbiviimise ajal ei peetud seega kõigis valitsemisala asutustes ajakohast ja terviklikku töötlemistoimingute registrit, mis sisaldanuks vastutava töötleja puhul GDPRi artikli 30 lõikes 1 ning volitatud töötlejana tegutsemise korral artikli 30 lõikes 2 nõutud teavet. Seetõttu ei ole asutustel võimalik järjepidevalt tõendada artikli 30 nõuete täitmist ning see piirab ka artikli 5 lõikes 2 sätestatud vastutuse põhimõtte täitmise tõendamist. Töö läbiviimise ajal tuvastatud puudused ei ole kõigis valitsemisala asutustes kõrvaldatud. Kuna töötlemistoimingute register on oma olemuselt ajas muutuv töövahend, tuleb seda töötlemistoimingute muutumisel järjepidevalt täiendada ja ajakohastada; **tegemist ei ole ühekordselt valmiva dokumendina**.

JÄRELDUS 18 — ülevaadete sisuline täielikkus ja detailsus. Asutustes, kus töötlemisülevaade on olemas, sisaldavad need olulises osas GDPRi artiklis 30 nõutud andmeid, kuid nende detailsus ja täielikkus on ebaühtlane.

TRAMi isikuandmete töötlemistoimingute ülevaade ei ole täielikult kooskõlas GDPR artikli 30 lõikest 1 tulenevate nõuetega. 7 juhul 16st puudus töötlemistoimingu juures kohustuslik töötlemise eesmärgi kirjeldus ning 33 juhul 180-st ei olnud esitatud GDPR artikli 30 lõike 1 punktis g nõutud tehniliste ja korralduslike turvameetmete üldist kirjeldust. Lisaks esines puudusi vabatahtlikult esitatavates andmeväljades: kõikide töötlemistoimingute puhul ei olnud määratud säilitustähtaega ega õiguslikku alust, eriliigiliste isikuandmete töötlemine ei olnud järjepidevalt eristatud ning vastutava ja volitatud töötleja rollid ei olnud ülevaates üheselt määratletud, mistõttu ei taga TRAMi töötlemistoimingute ülevaade täielikku ja üheselt mõistetavat ülevaadet organisatsiooni isikuandmete töötlemisest.

KeA isikuandmete töötlemistoimingute ülevaates vajavad personaliteenuse ning asjaajamise ja dokumendihalduse koondkirjed täpsustamist, et töötlemise eesmärgid, andmesubjektide kategooriad ja isikuandmete liigid oleksid GDPRi artikli 30 lõike 1 punktide b ja c kohaselt üheselt tuvastatavad. Samuti ei ole ülevaates selgelt eristatud KeA tegevust vastutava ja volitatud töötlejana. Lisaks on ülevaates ebaühtlaselt kajastatud mõningat KeA enda praktiliseks kasutamiseks lisatud teavet, sh töötlemise õiguslikke aluseid, vastutavaid struktuuriüksusi, kasutatavaid infosüsteeme ja viiteid alusdokumentidele. Viimati nimetatud teave ei kuulu GDPRi artikli 30 kohustuslike registriväljade hulka. Selle ühtlasem kajastamine parandaks ülevaate arusaadavust ja kasutatavust, kuid teabe ebaühtlane kajastamine ei tähenda iseenesest GDPRi artikli 30 nõuete rikkumist.

KeMITi ülevaade hõlmab nii vastutava kui ka volitatud töötleja rolli ning sisaldab olulises osas nõutud andmeid, kuid volitatud töötleja andmete täpsus sõltub osaliselt teiste asutuste esitatud teabest. KeMIT/RIT peab volitatud töötlejana ise pidama registrit vastutavate töötlejate nimel tehtavate töötlemistoimingute kategooriate kohta, kuid vastutavad töötlejad peavad andma KeMIT/RITile piisava info, et ta saaks seda kohustust sisuliselt täita.

Puudulik või liiga üldine dokumenteerimine vähendab ülevaadete kasutusväärtust ning võib raskendada asutuse suutlikkust tõendada töötlemise õiguspärasust, eesmärgipärasust, säilitamise põhjendatust ja rakendatud turvameetmete asjakohasust.

JÄRELDUS 19 — töötlemisülevaadete koostamise vastutus ja ajakohastamise korraldus. Töötlemisülevaate pidamise ja ajakohasuse tagamise eest vastutab asutus kui vastutav töötleja. Ülevaate koostamist koordineerib asutustes üldjuhul AKS, kelle ülesanne on nõustada, toetada ja seirata isikuandmete kaitse nõuete täitmist, kuid töötlemistoimingute sisulise õigsuse ja ajakohasuse tagamine eeldab valdkondlike üksuste, teenuseomanike, protsessiomanike ning teiste valdkondlike vastutajate osalemist.

TRAMis vastutavad andmete ajakohasuse eest teenusejuhid, KeAs teenuseomanikud ja RiLis üksuste juhid. KliMis on ülevaate koostamine korraldatud koostöös struktuuriüksuste või sisuosakondadega ning KAURis teenuste omanike, sh alamteenuste omanike, valdkondlike üksuste ja teiste asjaomaste vastutajatega. Selline asutusesisene tööjaotus toetab ülevaate sisulist kvaliteeti, sest AKSil ei pruugi olla täielikku teadmist kõigist tööprotsessidest, kuid ei muuda asutuse kui vastutava töötleja vastutust tagada, et ülevaade vastab GDPRi artikli 30 nõuetele ja on ajakohane.

KliMis, KAURis, RiLis ja EGTs on töötlemisülevaadete koostamise edenemist aeglustanud struktuuriüksustelt sisendi kogumise ajamahukus, töö suur maht, tööprotsesside keerukus ning vajadus juhendada üksusi isikuandmete töötlemistoimingute tuvastamisel ja kirjeldamisel. KAUR on töö lõpuleviimiseks kaasanud välise teenusepakkuja, kelle ülesanne on 08.09.2026 sõlmitud lepingu kohaselt kaardistada asutuse isikuandmete töötlemise toimingud ning koostada töötlemisülevaade ja töö aruanne hiljemalt 12.11.2026. EGTs oli ülevaate edasiarendamine kavandatud 2026. aastasse.

KeMITi ülesannete ümberkorraldamisel ja jaotamisel Riigi Digikeskuse, RIA ning KliMi vahel tuleb asjaomastel asutustel ajakohastada töötlemisülevaateid ulatuses, milles muutuvad isikuandmete töötlemisega seotud rollid, töötlemistoimingud, vastuvõtjate kategooriad või volitatud töötlejana tehtavate töötlemistoimingute kategooriad.

Ülevaadete nõuetekohase seisu saavutamiseks ja ajakohasena hoidmiseks on vajalik tagada struktuuriüksuste sisuline panus ja juhtkonna tugi, määrata vastutavad isikud, rakendada ühtset metoodikat, kehtestada realistlik ajakava ja ajakohastamise kord ning eraldada tööks piisav ressurss. KAURi puhul vähendab teenusepakkuja kaasamine töö viibimise riski, kuid ülevaate sisuline täielikkus ja edasine ajakohastamine sõltuvad endiselt asutuse üksuste panusest, tulemuste vastuvõtmisest ning püsiva vastutuse ja ajakohastamise korra määramisest.

Samas ei taga osapoolte kaasamine iseenesest ülevaate ajakohasust: ilmnes, et muudatustest teavitamine ja andmete valideerimine ei toimi alati õigel ajal ning ajakohastamise kord ei ole kõigis asutustes piisavalt dokumenteeritud. Kui teenuseomanike, valdkondlike üksuste ja teiste asjasse puutuvate vastutajate kohustus teavitada AKSi töötlemistoimingute muudatustest ning ülesanded andmete kinnitamisel ja perioodilisel ülevaatamisel ei ole selgelt määratud, võib ülevaate ajakohastamine jääda sõltuma AKSi meeldetuletustest või üksuste vabatahtlikust sisendist ning suureneb risk, et töötlemistoimingute ülevaade ei kajasta tegelikku isikuandmete töötlemise olukorda ja see võib piirata asutuste suutlikkust tõendada GDPRi artikli 30 kohase dokumenteerimiskohustuse ja artikli 5 lõikes 2 sätestatud vastutuse põhimõtte täitmist.

JÄRELDUS 20 — vastutavate ja volitatud töötlejate vaheline infovahetus. KliM valitsemisalas ei ole kogutud teabe põhjal kujunenud järjepidevat ega süsteemset praktikat isikuandmete töötlemisülevaadete ja kaardistuste jagamiseks vastutavate töötlejate (KliM, KeA, KAUR, RiL, EGT ja ELM) ning KeMITi kui mitmele asutusele IT-teenuseid osutava volitatud töötleja vahel. KeMITi hinnangul puudub seetõttu terviklik ülevaade sellest, milliseid isikuandmeid erinevates süsteemides ja andmekogudes töödeldakse, millised andmekategooriad seal esinevad ning millised riskid ja turvameetmed on asjakohased. Ebapiisav infovahetus võib raskendada intsidentide käsitlemist, sobivate turvameetmete määratlemist ja riskijuhtimist ning põhjustada olukordi, kus andmete tegelik koosseis ja ulatus selgub alles intsidendi või muu probleemi ilmnemisel.

ETTEPANEK kõikidele asutustele:

23. Määrata isikuandmete töötlemise ülevaate koostamise, haldamise ja ajakohastamise korraldus selliselt, et selles oleksid selgelt kirjeldatud AKSi, struktuuriüksuste, teenuseomanike, protsessiomanike ja vajaduse korral infovara omanike rollid. Korras või töökorralduslikus juhises tuleks määrata, millal tuleb uuest või muutunud töötlemistoimingust AKSile teatada, kes vastutab töötlemistoimingu sisulise kirjelduse õigsuse eest, kui sageli ülevaadet üle vaadatakse ning kuidas dokumenteeritakse muudatused ja versioonid.

ETTEPANEK KliMile, KAURile, RiLile, EGTle ja ELMile:

24. **Viia isikuandmete töötlemisülevaade asutuses tehtud töö valmidusastmest lähtudes sellisesse seisu, kus kõik asutuse teadaolevad töötlemistoimingud on nõutud ulatuses dokumenteeritud, andmed sisuliselt kontrollitud ning ülevaate edasine ajakohastamine püsivalt korraldatud**. Ülevaade peab hõlmama asutuse vastutusel tehtavaid isikuandmete töötlemistoiminguid ning sisaldama GDPRi artikli 30 lõikes 1 nõutud teavet, sh töötlemise eesmärke, andmesubjektide kategooriate ja isikuandmete liikide kirjeldust, vastuvõtjate kategooriaid ning kolmandatele riikidele või rahvusvahelistele organisatsioonidele edastamise korral asjakohaseid andmeid. Võimaluse korral tuleb ülevaates märkida eri andmeliikide kustutamiseks ette nähtud tähtajad ning esitada GDPRi artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus. Kustutamistähtaegade kajastamisel kasutada asutuse dokumentide loetelus, liigitusskeemis või muus teabehalduse alusdokumendis määratud säilitustähtaegu või viidata neile viisil, mis võimaldab tähtaja üheselt kindlaks teha. **Samuti tuleb tagada, et oleksid asjakohasel juhul asutuse rollide kaupa selgelt eristatud**

vastutava töötlejana tehtavad isikuandmete töötlemistoimingud ja vastutava töötleja nimel volitatud töötlejana tehtavate töötlemistoimingute kategooriad. KeMITi ülesannete ümberkorraldamisel ja jaotamisel Riigi Digikeskuse, RIA ning KliMi vahel tuleb asjaomastel asutustel ajakohastada töötlemisülevaateid ulatuses, milles muutuvad isikuandmete töötlemisega seotud rollid, töötlemistoimingud, vastuvõtjate kategooriad või volitatud töötlejana tehtavate töötlemistoimingute kategooriad.

a. KliMil viia lõpule isikuandmete töötlemise ülevaatesse kogutud andmete valideerimine ja täpsustamine ning määrata selleks tähtaeg. Edaspidi jätkata ülevaate jooksva ajakohastamise ja muudatuste dokumenteerimise töökorralduse rakendamist.
b. KAURil tagada lepingu alusel valmiva töötlemisülevaate edasine ajakohastamine.
c. RiLil viia töötlemisülevaate koostamine lõpule, kaasates andmete täpsustamisse ja valideerimisse üksuste juhid, ning edaspidi rakendada kavandatud töökorraldust, mille kohaselt vastutab AKS ülevaate pideva ajakohastamise eest ja üksuste juhid edastavad muudatused jooksvalt.
d. **EGTl määrata juhtkonna tasandil isikuandmete töötlemistoimingute kaardistamise tähtaeg ülevaadete nõuetekohase seisu saavutamiseks**, kaardistamise korraldamise eest vastutav isik. Dokumenteerida töötlemistoimingud asutuse vajadustele sobivas vormis või infosüsteemis viisil, mis tagab teabe terviklikkuse, võrreldavuse, leitavuse ja ajakohastatavuse. Tagada edaspidine ajakohastamine.
e. **ELMil määrata juhtkonna tasandil isikuandmete töötlemistoimingute kaardistamise tähtaeg ülevaadete nõuetekohase seisu saavutamiseks**, kaardistamise korraldamise eest vastutav isik. Dokumenteerida töötlemistoimingud asutuse vajadustele sobivas vormis või infosüsteemis, mis tagab teabe terviklikkuse, võrreldavuse, leitavuse ja ajakohastatavuse. Tagada edaspidine ajakohastamine.

ETTEPANEK TRAMile, KeAle ja KeMITile:

25. Ajakohastada ja täiendada isikuandmete töötlemise ülevaateid selliselt, et töötlemistoimingud oleksid kirjeldatud piisava detailsusega ning ülevaadetes oleksid selgelt ja eristatavalt kajastatud töötlemise eesmärgid, andmesubjektide ja isikuandmete kategooriad, andmete vastuvõtjate kategooriad, kavandatud säilitustähtajad, vajaduse korral turvameetmete üldine kirjeldus ning avaliku teabe režiim. Lähtudes töötlemisega kaasnevatest riskidest ja vastutustundlikkuse põhimõttest, tagada, et ülevaadetest oleks üheselt tuvastatav eriliigiliste isikuandmete ning süüteoasjades tehtud süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemine, ilma et nende andmete kajastamiseks oleks tingimata vaja luua eraldi välja. Ülevaadete ajakohastamisel pöörata erilist tähelepanu teenuse- ja protsessipõhiste koondkirjete täpsustamisele, et nende põhjal oleks võimalik tuvastada konkreetsed töötlemistoimingud, nendega seotud andmekaitseriskid ja vastutus. Täiendada töötlemise ülevaateid volitatud töötlejana tehtavate töötlemistoimingute kategooriatega, tuues iga sellise toimingu puhul selgelt välja vastutava töötleja, kelle nimel asutus tegutseb, et asutuse roll ja sellest tulenevad kohustused oleksid üheselt arusaadavad, ning tagada ülevaadete järjepidev ajakohastamine, sh juhul, kui lisandub uusi vastutavaid töötlejaid või nende nimel tehtavate töötlemistoimingute kategooriaid.

ETTEPANEK KliMile, KeAle, KAURile, RiLile, EGT-le ja ELMile koostöös KeMITi ja RITiga (edaspidi arvestades ümberkorraldusi Riigi Digikeskuse, RIA ja KliM vahel):

26. KliMil algatada KliMi valitsemisala asutuste ning KeMITi ja RiTi asjaomaste esindajate ühine arutelu, et hinnata IT-teenuste osutamisega seotud teabevahetuse põhimõtteid, protsesse, menetlusi, dokumentatsiooni, suhtluskanaleid ja kontaktpunkte ning leppida kokku nende vajalikus täiendamises. KeMITil ja RITil koordineerida kumbki enda osutatavate teenuste ulatuses koostöös KliMi ja teenindatavate asutustega teabevahetuse praktilise korralduse väljatöötamist.
    Koostöös hinnata, millistes teenuse tellimise, arendamise, muutmise ja haldamise protsessides kogutakse ning edastatakse IT-teenuse osutajale tema ülesannete täitmiseks vajalik teave, ja määrata, milline teave, millises etapis, millise kanali kaudu ning millise regulaarsusega edastatakse. **Teabevahetus peab tagama, et IT-teenuse osutajal oleks IT-teenuse osutaja ja isikuandmete volitatud töötleja ülesannete täitmiseks piisav ning ajakohane teave mh hallatavates või toetatavates infosüsteemides töödeldavatest isikuandmetest, andmekategooriatest, vastutavatest töötlejatest, andmevoogudest ja turvameetmete vajadusest**.
    Samuti tuleb määrata osaliste ülesanded ja vastutus ning lõimida teabe edastamine teenuse tellimise, arendamise ja muudatuste kavandamise protsessidesse. Teabevahetuse korraldus peab hõlmama nii kavandatavaid teenuseid ja muudatusi kui ka teabe hilisemat regulaarset ajakohastamist ning uutest või muutunud isikuandmete töötlemistoimingutest ja infosüsteemidest teavitamist. **AKSid tuleb kaasata isikuandmete kaitse nõudeid puudutavates küsimustes nõustavasse rolli, kuid IT-teenuste tellimise, dokumenteerimise ja teabevahetuse protsesside koordineerimine ei peaks jääma AKSide ülesandeks**.
    Selline korraldus toetab intsidentide kiiremat lahendamist, turvameetmete täpsemat kavandamist ja valitsemisala riskijuhtimist. KeMITi ülesannete ümberkorraldamisel tuleb koostöös uute teenuseosutajatega seada eesmärgiks samade teabevahetuspõhimõtete rakendamine uues teenusekorralduses ning määrata selgelt asjaomased protsessid, vastutajad, suhtluskanalid ja kontaktpunktid.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*
KliM	Töötlemisülevaate ajakohastamine on KliMi AKSi tööplaanis kõrgel kohal, kuid selle koostamise tempot mõjutab muude jooksvate ülesannete ja projektide maht. Töö töötlemisülevaatega toimub järk-järgult. Plaanis on olemasolev ülevaade tervikuna üle vaadata, teha sisuosakondadega koostööd andmete valideerimiseks ja täpsustamiseks ning viia ülevaate koostamine lõpuni. Töötlemisülevaatesse kogutud andmete valideerimise ja täpsustamise tähtajaks seame 2027. aasta esimese kvartali lõpu. Lisaks on plaanis hinnata, kas töötlemisülevaate pidamiseks oleks võimalik Exceli asemel kasutada mõnda efektiivsemat keskkonda või süsteemi. Koostatavas isikuandmete töötlemise korras on kavas kirjeldada ka töötlemisülevaate edaspidise ajakohastamise põhimõtted ja kord, et tagada selle regulaarne ülevaatamine ja ajakohasus. Samuti on eesmärk üle vaadata KliMi, valitsemisala asutuste ja IT-teenuse osutajate vahelise teabevahetuse korraldus. Selle tegevuse ajastamisel tuleb aga arvestada käimaolevate asutuste ümberkorraldustega. **Nõustume ettepanekuga 26**. KliM algatab Riigi Digikeskuse, RIA ja KliMi valitsemisala asjaomaste asutustega ühise arutelu, et leppida kokku IT-teenuste osutamisega seotud teabevahetuse korraldus. Selleks vaadatakse üle olemasolevad kokkulepped ning valmistatakse ette nende vajalikud muudatused või uued lepingud. **Olemasolevate lepingute muudatused või uued lepingud sõlmitakse pärast KeMITi ülesannete ümberkorraldamise lõpuleviimist, lähtudes ümberkorraldamise tulemusena kujunenud ülesannete ja vastutuse jaotusest**. Kokkulepetes määratakse edastatava teabe koosseis, edastamise etapid ja kanalid, ajakohastamise kord, osaliste ülesanded ja vastutus, vastutajad ja kontaktpunktid ning kokkulepitud korralduse rakendamise tähtajad. Samuti määratakse, kuidas lõimitakse teabevahetus teenuste tellimise, arendamise, muutmise ja haldamise protsessidesse. Kokkulepped hõlmavad ka teenuseosutajale isikuandmete volitatud töötleja ülesannete täitmiseks vajaliku teabe edastamist ulatuses, milles teenuseosutaja neid ülesandeid täidab. AKSid kaasatakse isikuandmete kaitse nõudeid puudutavates küsimustes nõustavasse rolli; protsesside koordineerimine jääb nende eest vastutavate osaliste ülesandeks.
TRAM	**Kommentaar ettepaneku punktile 23**: Asutuses on tööprotsesse kirjeldavate kordade ja juhendite ülevaatamine reguleeritud asutuse teenuste dokumentide korras, mille kohaselt hindab teenusejuht dokumentide ajakohastamise vajadust vähemalt üks (1) kord aastas. Lisaks on 03.09.2026 kinnitatud isikuandmete töötlemise korras sätestatud, et töötlemistoimingute registrit peab AKS koostöös struktuuriüksuse juhiga, sisendi annab isikuandmeid töötlev struktuuriüksus või asjakohasel juhul infosüsteemi peakasutaja. Registri ajakohasuse eest vastutab töötlemistoimingu eest vastutav struktuuriüksus ning kirjeid ajakohastatakse töötlemistoimingute lisandumisel või muutumisel. Leiame, et kehtestatud töökorraldus loob aluse töötlemisülevaate järjepidevaks ajakohastamiseks ning vastutuse jaotamiseks. **Kommentaar ettepaneku punktile 25**: Nõustume, et töötlemisülevaade peab andma piisavalt detailse ja üheselt mõistetava ülevaate isikuandmete töötlemistoimingutest ning kajastama GDPRi artiklis 30 nõutud teavet. Asutuse AKS ajakohastab praegu töötlemisülevaate tabelit, et viia see vastavusse nimetatud artikli nõuetega. Seejärel saavad teenusejuhid ülevaate täiendamiseks ning töötlemistoimingute täpsemaks kirjeldamiseks. Täiendamisel pööratakse tähelepanu ka eriliigiliste isikuandmetega seotud isikuandmete töötlemise selgele kajastamisele, samuti volitatud töötlejana tehtavate toimingute ja vastutavate töötlejate määratlemisele. Ettepanekus toodud nõue kajastada süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemist ilma eraldi välja loomise kohustuseta vajab meie hinnangul täiendavat selgitamist, eelkõige selles osas, millist kajastamisviisi peetakse piisavaks, et töötlemine oleks ülevaatest üheselt tuvastatav. **Audiitori täiendav selgitus:** Ettepanekus 25 peetakse silmas, et kui töötlemistoiming hõlmab süüteoasjades tehtud süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmeid, oleks see asjaomase töötlemistoimingu juures selgelt ja üheselt märgitud. Soovitus tugineb GDPRi artikli 30 lõike 1 punktis c sätestatud isikuandmete liikide kirjeldamise kohustusele ning artikli 5 lõikes 2 sätestatud vastutuse põhimõttele, arvestades artikli 24 lõikes 1 ette nähtud riskipõhist lähenemist töötlemise nõuetekohasuse tagamisele ja tõendamisele. Nende andmete töötlemise selge kajastamine aitab hinnata toiminguga seotud andmekaitseriske ja kohaldatavate nõuete, sealhulgas GDPRi artiklis 10 sätestatud töötlemistingimuste täitmist. Asutuse töötlemisülevaate praegust ülesehitust arvestades saab vastavad andmeliigid märkida veergu „Isikuandmete liigid“, nimetades näiteks andmed

	süüdimõistmise või määratud karistuse kohta. Veergudes „Teenuse nimi“ ja „Töötlemise eesmärk“ esitatud teave peab koos andmeliikide kirjeldusega võimaldama üheselt tuvastada, millise konkreetse töötlemistoimingu raames neid andmeid töödeldakse. Kui teenusepõhine koondkirje hõlmab mitut töötlemistoimingut ning nimetatud andmeid töödeldakse üksnes mõne toimingu raames, tuleb kirjet täpsustada nii, et see seos oleks eristatav, näiteks täpsustades olemasolevate veergude sisu või kajastades asjaomase toimingu eraldi real. Ettepaneku täitmisel peetakse piisavaks kajastamisviisi, millest selgub üheselt nii nimetatud andmete töötlemine kui ka asjaomane töötlemistoiming. Üksnes üldnimetusest, näiteks „menetlusandmed“, ei piisa juhul, kui kirje ülejäänud sisust ei selgu, et toiming hõlmab ka nimetatud andmeid. Ülevaates kirjeldatakse andmeliike, mitte konkreetsete isikute süüteo- või karistusandmeid. Viidatud GDPRi sätted ei nõua nende andmete kajastamiseks eraldi välja või veeru loomist ega näe ette kindlat vormistuslahendust. Asutus saab valida oma ülevaate ülesehitusega sobiva kajastamisviisi; soovituse eesmärk on tagada ülevaate sisuline selgus ning toetada andmekaitseriskide hindamist ja nõuetele vastavuse tõendamist, mitte kehtestada kohustuslikku vormistusviisi.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Isikuandmete töötlemise ülevaate korraldus reguleeritakse isikuandme kaitse korras, millise tähtajad ja vastutaja on toodud ülal.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	Nõus ettepanekuga. Hetkel põhiprobleem, et meil puudub vastutavate töötlejate sisend, kus nad päriselt isikuandmeid töötlevad (oma töötlemise ülevaadet on jaganud ainult Kliimaministeerium). Seega KeMIT-i enda ülevaade on tõenäoliselt ebatäpne.
EGT	EGT nõustub töötlemisülevaate täiendamise ja ajakohastamise vajadusega. Töö eeldab struktuuriüksuste sisulist panust ning vastutust oma töötlemistoimingute kirjelduste õigsuse eest. Juhtkonna tasandil tuleb kokku leppida realistlik ajakava, ülesannete jaotus ja tööks vajalik ressurss.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud. AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

4. Mõjuhinnangud

Lähtekoht: Asutuses peab olema dokumenteeritud andmekaitsealase mõjuhinnangu (DPIA) vajaduse hindamise, koostamise, ajakohastamise ja tulemuste rakendamise korraldus, mis tagab, et enne uue või oluliselt muudetud isikuandmete töötlemise toimingu, infosüsteemi või teenuse kasutuselevõttu hinnatakse töötlemisega kaasnevat ohtu füüsiliste isikute õigustele ja vabadustele ning suure ohu tõenäosuse korral koostatakse enne töötlemise alustamist DPIA. Määratud peavad

olema vastutajad ja kaasatavad rollid ning DPIA peab sisaldama vähemalt kavandatud töötlemistoimingute ja nende eesmärkide, sh asjakohasel juhul vastutava töötleja õigustatud huvi süstemaatilist kirjeldust, töötlemise vajalikkuse ja proportsionaalsuse hinnangut, andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnangut ning ohtude käsitlemiseks kavandatud meetmeid, sh tagatisi, turvameetmeid ja mehhanisme isikuandmete kaitse tagamiseks ning GDPRi nõuete täitmise tõendamiseks

JÄRELDUS 21 — mõjuhinnangute koostamise korraldus, rollid ja vastutus ei ole kõigis asutustes piisavalt selgelt dokumenteeritud. KliM valitsemisala asutustes on andmekaitsealaste mõjuhinnangute vajaduse hindamise, koostamise ja dokumenteerimise korraldus ning sellega seotud rollide ja vastutuse määratlemine ebaühtlane. Andmekaitsealase **mõjuhinnangu tegemise eest vastutab vastutav töötleja**. Protsessi- või teenuseomanik peab kirjeldama kavandatavat andmetöötlust ja sellega seotud riske, algatama mõjuhinnangu vajaduse hindamise ning vajaduse korral korraldama mõjuhinnangu tegemise. **AKS nõustab ja jälgib mõjuhinnangu toimimist, kuid tema roll ei asenda vastutava töötleja ega protsessi- või teenuseomaniku sisulist vastutust**.

TRAMis ja KeMITis on mõjuhinnangute koostamise põhimõtted ja asjaomased rollid sätestatud kehtivas asutusesiseses korras ning TRAMis toetavad protsessi ka mõjuhinnangu vormid ja juhend.

KliMis ja KeAs on mõjuhinnangute põhimõtted ning asjaomased rollid kavandatud koostamisel olevates isikuandmete kaitse kordades, kuid need ei olnud töö läbiviimise ajal veel kehtestatud.

RiL kavandab mõjuhinnangute käsitlemist koostatavas isikuandmete kaitse korras. Praktikas toimub hindamine AKSi ja protsessiomaniku koostöös, kuid protsessi- või teenuseomaniku vastutus hindamise algatamise ja vajaliku teabe esitamise eest ei ole dokumentides üheselt fikseeritud.

KAURis ja EGTs ei ole iseseisvalt kehtestatud raamistikku ning asutused on viidanud KliMi võimaliku korra ootamisele või selle sobivuse hindamisele.

KAURis, EGTs ja ELMis ei ole määratud ametikohta või üksust, kes vastutab mõjuhinnangu vajaduse hindamise algatamise ja mõjuhinnangu tegemise korraldamise eest.

ELMis ei ole DPIA läbiviimise korda ega rollijaotust kehtestatud ning asutus ei ole seni eraldi korra vajadust arutanud.

KeA Logify näide kinnitas, et protsessi- ja teenuseomanike vastutus ei ole olnud piisavalt selgelt määratletud ega teadvustatud; koostatavas isikuandmete kaitse korras vastutust täpsustatakse.

Kuigi GDPR ei nõua kõigis asutustes ühesugust vormi või protsessi, peab iga vastutav töötleja tagama, et kõrge riskiga isikuandmete töötlemise korral hinnatakse DPIA vajadust, koostatakse mõjuhinnang ning dokumenteeritakse otsused ja riskide maandamise meetmed. Dokumenteerimata või ebaselge korraldus ja selgelt määramata vastutus suurendavad riski, et mõjuhinnangu vajadust ei tuvastata ega hinnata õigel ajal, hindamine jääb algatamata või mõjuhinnangu tegemine korraldamata.

JÄRELDUS 22 — vastutava ja volitatud töötleja koostöö ning mõjuhinnanguga seotud teabevahetus ei ole alati piisavalt selgelt korraldatud. Valitsemisala asutused kasutavad ühiseid infosüsteeme ning IT- ja tugiteenuseid, mille osutamisel peab vastutav töötleja hindama mõjuhinnangu vajadust, tegema vajaduse korral mõjuhinnangu ja määrama riskide maandamise meetmed. Volitatud töötleja peab vastutavat töötlejat toetama töötlemise laadi ja talle kättesaadava teabe ulatuses.

KeMIT tegutseb oma tööprotsessides vastutava töötlejana ning teiste asutuste infosüsteemide ja IT-teenuste puhul sõltuvalt töötlemise korraldusest volitatud töötlejana, kuid tema esitatud teabe kohaselt vastutavate töötlejate koostatud või kavandatavate mõjuhinnangute teave ei jõua alati temani. RiLi kirjeldatud RTK personali- ja palgaarvestuse teenuse näide osutab, et ühiste tugiteenuste kasutamisel ei pruugi asutusel olla piisavat ülevaadet rollide ja vastutuse jaotusest ega asjakohastest dokumentidest, kui valitsemisalaülesed kokkulepped ei ole kättesaadavad või nende sisu ei ole tutvustatud. TRAM[3], KeA ja KAUR täidavad andmekogude põhimääruste alusel ka volitatud töötleja ülesandeid, samas võib tulevikus lisanduda uusi andmekogusid või muid isikuandmete töötlemise tegevusi. Nii praegustele kui ka võimalikele tulevastele volitatud töötleja ülesannetele tuleb kohaldada samu koostöö- ja teabevahetuspõhimõtteid ning tagada samade kohustuste järjepidev täitmine.

KeMITi ümberkorraldamisel ning selle ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliM vahel tuleb uues teenusekorralduses selgelt kokku leppida mõjuhinnanguteks vajaliku tehnilise ja korraldusliku teabe vahetamine, osapoolte abistamiskohustused ning teenindatavate asutuste AKSide kaasamine. Puudulik koostöö ja teabevahetus suurendab riski, et mõjuhinnangud ei hõlma kõiki töötlemisega seotud süsteeme, teenuseid, osalisi ja asjaolusid, andmekaitseriske hinnatakse osaliselt või hilinenult ning vajalikud tehnilised ja korralduslikud kaitsemeetmed jäävad kavandamata või õigel ajal rakendamata.

[3] TRAM on andmekogude põhimääruse kohaselt liiklusjärelevalve infosüsteemi ja sadamaregistri volitatud töötleja. Mõlema andmekogu vastutav töötleja on KliM.

JÄRELDUS 23 — mõjuhinnangu vajaduse hindamist ei algatata ja asutusesiseseid osalisi ei kaasata alati piisavalt vara. GDPRi artikli 35 lõike 1 kohaselt tuleb mõjuhinnang teha **enne** sellise isikuandmete töötlemise alustamist, millega tõenäoliselt kaasneb suur oht füüsiliste isikute õigustele ja vabadustele, ning etapis, kus selle tulemusi saab veel arvestada töötlemise eesmärkide, andmekoosseisu, tehniliste lahenduste ja kaitsemeetmete kujundamisel. Nagu eespool kirjeldatud, vastutab mõjuhinnangu vajaduse hindamise ja vajaduse korral mõjuhinnangu tegemise eest vastutav või kaasvastutav töötleja. Asutusesiseselt peab hindamise algatama ja korraldama asjaomase töötlemise eest vastutav protsessi- või teenuseomanik, kaasates õigel ajal AKSi ning vajalikud IT-, infoturbe- ja õigusvaldkonna esindajad.

TRAMis saab AKS võimalikust mõjuhinnangu vajadusest sageli teada arenduse hilises etapis või pärast infosüsteemi kasutuselevõttu. KliMis on AKSi kaasamine süsteemsem õigusloomeprotsessides, kuid mitte alati muudes isikuandmete töötlemisega seotud tegevustes, näiteks uuringutes. KAURi GPS-seadmete kasutamise näide osutas samuti vajadusele hinnata tehniliste jälgimislahenduste puhul mõjuhinnangu vajadust süsteemselt, õigel ajal ja dokumenteeritult.

AKSid tõid välja, et mitme infosüsteemi puhul oleks mõjuhinnangu vajadust tulnud hinnata ajal, mil allasutustes ei olnud AKSi roll veel asutusepõhiselt korraldatud. AKSi rolli hilisem asutusepõhine korraldamine ei kõrvaldanud ega muutnud siiski asutuse kui vastutava või kaasvastutava töötleja kohustust hinnata mõjuhinnangu vajadust ja vajaduse korral mõjuhinnang teha. Seetõttu ei saa enne AKSi rolli delegeerimist tegemata jäänud hindamisi või mõjuhinnanguid käsitada hiljem määratud AKSi tegevuse puudusena, kuid need jäävad asjaomase asutuse kui vastutava või kaasvastutava töötleja kohustuse täitmise küsimuseks.

Mõjuhinnangu vajaduse hiline hindamine ja asjaomaste osaliste hiline kaasamine võib jätta andmekaitseriskid enne töötlemise alustamist tuvastamata ning muuta vajalike muudatuste tegemise keerukamaks, kulukamaks ja ajamahukamaks.

JÄRELDUS 24 — mõjuhinnangu vajaduse hindamise ja tehtud mõjuhinnangute läbivaatamise dokumenteeritus ei ole alati olnud tagatud. Kogutud teabe põhjal ei olnud KliMil, KeAl, RiLil, KeMITil, EGTl ja ELMil terviklikku dokumenteeritud ülevaadet töötlemistoimingutest, mille puhul on hinnatud andmekaitsealase mõjuhinnangu vajadust, hindamise tulemustest ja põhjendustest ning tehtud või töötlemisega kaasneva ohu muutumisel läbi vaadatud mõjuhinnangutest.

KliMis, KeAs, RiLis, EGTs ja ELMis ei ole perioodil 01.07.2023–31.12.2025 tehtud GDPRi artikli 35 kohaseid mõjuhinnanguid. KliMis on isikuandmete töötlemisega kaasnevaid mõjusid käsitletud eelnõude ja arendusprojektide üldisemates analüüsides. KeA on 2026. aastal koostanud ATK 2.0 riskihindamise käskkirja. KeA Logify näide osutas, et andmekaitsealane riskianalüüs või mõjuhinnangu vajadus võib esile kerkida alles pärast süsteemi kasutuselevõttu. KAUR hindas mõjuhinnangu vajadust PISTRIKU arendamisel, mis hakkab KliMi selgituse kohaselt toimima KOTKASe alamsüsteemina (*KOTKASe põhimääruse muutmisel määratakse kaasvastutavateks töötlejateks KeA ja KAUR ning kaasvastutavaks töötlejaks PISTRIKU osas saab olema KAUR*). PISTRIKU arendamise, KOTKASe pilvekeskkonda viimise ja KIRKE välisvõrku viimise puhul soovitas KliM AKS kaaluda mõjuhinnangu tegemist, kuid mõjuhinnanguid ei tehtud. KeMIT ei ole veel hinnanud ega dokumenteerinud mõjuhinnangu vajadust tema vastutusel olevate süsteemide, näiteks e-posti süsteemi töötlemistoimingute puhul. TRAMi AKS analüüsis koos merendus- ja liiklusosakonna struktuuriüksustega olemasolevaid mõjuhinnanguid ja uute mõjuhinnangute vajadust samaaegselt valdkondlike infosüsteemide ja andmekogude põhimääruste ülevaatamisega. Lisaks alustas TRAM liiklusregistri test- ja arenduskeskkonna mõjuhinnangu tegemist pärast seda, kui AKI algatas TRAMi suhtes järelevalvemenetluse, kuna keskkonnas kasutatakse tegelikke isikuandmeid.

Kogutud teabe põhjal ei olnud kõigis asutustes piisavalt jälgitav, kas mõjuhinnangu vajadust hinnatakse süsteemselt ja põhjendatult, kuidas dokumenteeritakse otsus mõjuhinnangu tegemise või tegemata jätmise kohta ning kas tehtud mõjuhinnang vaadatakse vajaduse korral läbi. See piirab GDPRi artikli 35 nõuete täitmise ja artikli 5 lõikes 2 sätestatud vastutustundlikkuse põhimõtte järgimise tõendatavust.

ETTEPANEKUD kõikidele asutustele:

27. Tagada, et asutuses oleks dokumenteeritud DPIA vajaduse hindamise ja mõjuhinnangu koostamise miinimumprotsess. Protsess peaks kirjeldama, millal tuleb hinnata DPIA vajadust, kes algatab hindamise, millal ja kuidas kaasatakse AKS, protsessiomanik, IT/infoturbe, õigusvaldkond ja vajaduse korral volitatud töötleja, kuidas dokumenteeritakse eelhinnang ning otsus DPIA koostamise või koostamata jätmise kohta, kuidas kinnitatakse ja säilitatakse mõjuhinnang ning millal seda ajakohastatakse. DPIA vajaduse hindamisel tuleks lähtuda GDPR artikli 35 lõikes 3 nimetatud olukordadest, GDPR artikli 35 lõike 4 alusel avaldatud AKI loetelust ning EDPB suunistes toodud kõrge riski kriteeriumidest. Protsess võib olla osa isikuandmete kaitse korrast, arendusprotsessist, riskijuhtimise korrast, muudatuste juhtimise korrast või eraldi juhis, kuid see peab olema teenistujatele ja protsessiomanikele arusaadav ja kättesaadav.

28. Lõimida DPIA vajaduse hindamine süsteemiarenduste, uuringute, tehniliste jälgimislahenduste, hangete, lepingute ja muude uute või muutuvate andmetöötluste varasesse kavandamisetappi. Enne isikuandmete töötlemise alustamist või olulise muudatuse rakendamist tuleks dokumenteerida, kas DPIA on vajalik, ning tagada AKSi ja vajaduse korral IT/infoturbe, õigusvaldkonna ja teenusepakkuja kaasamine. Eriti tuleks seda arvestada TRAMi infosüsteemide arendustes, KliMi uuringutes, KeA Logify-laadsetes lahendustes ning KAURi GPS- või muude tehniliste jälgimislahenduste puhul. Laiemas vaates tagada, et AKS kaasatakse infosüsteemide arendustesse ja muudesse uutesse või muutuvatesse isikuandmete töötlemist hõlmavatesse tegevustesse võimalikult varases etapis, et enne töötlemise alustamist või süsteemi kasutuselevõttu oleks võimalik hinnata andmekaitseriske ja vajaduse korral DPIA koostamise vajadust.

ETTEPANEK KliMile koostöös valitsemisala asutuste AKSidega:

29. Töötada välja valitsemisala asutustele kasutatav DPIA vajaduse hindamise abivahend või näidisprotsess, mida asutused saavad kohandada oma töökorraldusele. Abivahend võiks sisaldada eelhinnangu vormi, kriteeriume kõrge riski tuvastamiseks, juhiseid AKSi ja teiste rollide kaasamiseks, otsuse dokumenteerimise näidist, DPIA vormi ning juhiseid selle kohta, kuidas hinnata jääkriski ja millal tuleb kaaluda AKIga eelnevat konsulteerimist. See toetaks asutusi, kus DPIA praktikat ei ole veel välja kujunenud, ilma et KliM AKS võtaks üle vastutava töötleja otsustusvastutust.

ETTEPANEK KliMile, KeAle, KAURile, EGTle ja ELMile koostöös KeMITiga (edaspidi asjaomase asutusega):

30. Leppida arendus- ja teenuseprotsessides kokku, kuidas vastutav töötleja edastab asjaomasele IT-teenuse osutajale teabe DPIA vajaduse hindamise tulemustest ja koostatud mõjuhinnangutes tuvastatud tehnilistest või korralduslikest riskimaandamismeetmetest ulatuses, mis on vajalik IT-teenuse osutaja või volitatud töötleja rolli täitmiseks. Kokkuleppes tuleks käsitleda ka seda, kuidas selgitatakse arendusprojekti või teenuse muudatuse alguses välja, kas kavandatav lahendus hõlmab isikuandmete töötlemist, kas DPIA vajadust on hinnatud ning kas mõjuhinnang on vajaduse korral koostatud. Vastutav töötleja peab tagama, et IT-teenuse osutajale edastatakse piisav teave, et tehnilises lahenduses oleks võimalik arvestada tuvastatud andmekaitseriskide ja riskimaandamismeetmetega. KeMITi ümberkorraldamisel ning selle ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliMi vahel peaksid KliM ja teenindatavad asutused seadma eesmärgiks, et uue teenusekorralduse kujundamisel tagatakse senisega vähemalt samaväärne infovahetus ning teenindatavate asutuste AKSide õigeaegne kaasamine. Ülesannete ja vastutuse täpsustumisel tuleb koostöö- ja teenusedokumentides selgelt kokku leppida poolte pädevus, vastutus, infovahetuse korraldus ja teenusetingimused.

ETTEPANEK KliMile koostöös valitsemisala asutustega:

31. Tagada, et valitsemisala asutustel oleks ligipääs RTK osutatavate personali- ja palgaarvestuse teenustega seotud valitsemisalaülesele koostöökokkuleppele ning selge ülevaade teenusega seotud andmekaitsealastest rollidest, vastutusest ja dokumenteerimise korraldusest. Vajaduse korral tuleks koostada lühike selgitus, mis toetab asutusi nende töötajate andmete töötlemise riskide kaardistamisel ning DPIA vajaduse hindamisel.

ETTEPANEK TRAMile, KeAle, KAURile:

32. Kokku leppida ja rakendada TRAMis, KeAs ja KAURis põhimõtted ning töökorraldus (kaas)vastutava töötleja abistamiseks isikuandmete töötlemisega seotud riskide hindamisel ja andmekaitsealase mõjuhinnangu tegemisel. Määrata mh kindlaks asutuste ülesanded ja vastutajad, mõjuhinnangu vajadusele viitavate asjaolude tuvastamise ja (kaas)vastutavale töötlejale teatamise kord, vajaliku teabe sisu ja edastamise tähtajad ning tehtud toimingute dokumenteerimise nõuded. Põhimõtteid rakendada kõigi isikuandmete töötlemise toimingute suhtes, mille puhul asutus tegutseb volitatud töötlejana, sh uute andmekogude ja töötlemistoimingute lisandumisel.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*
KliM	Mõjuhinnangute koostamise osas on plaanis koostada eraldi juhis, mis toetaks töötajaid mõjuhinnangu vajaduse äratundmisel ning aitaks tagada AKSi õigeaegse kaasamise. Juhises on kavas käsitleda ka seda, kuidas tagada mõjuhinnangute ja andmekaitseriskidega seotud teabe õigeaegne jõudmine IT-teenuse osutajateni. Lisaks on eesmärk korrastada mõjuhinnangute koostamise protsessi tervikuna ning töötada välja selleks vajalikud dokumendivormid ja põhjad. Koostatavad materjalid, sealhulgas mõjuhinnangute juhis ja dokumendivormid, on plaanis kujundada selliselt, et neid oleks võimalik kasutada haldusalaüleselt. Samuti on oluline tõsta töötajate teadlikkust mõjuhinnangute vajadusest ja AKSi õigeaegsest kaasamisest läbi kavandatavate koolituste. Nõustume, et varasemate mõjuhinnangute puudumist ei saa käsitada hiljem ametisse määratud AKSi tegevuse puudusena.

	Nõustume ettepanekuga 30. Jätkame KeMITi ülesannete ümberkorraldamise raames Riigi Digikeskuse ja RIAga arutelusid, et tagada uues teenusekorralduses andmekaitsealase teabevahetuse järjepidevus ja teenindatavate asutuste AKSide õigeaegne kaasamine. Pärast ümberkorralduse toimumist sõlmime vajaliku ulatusega koostöö- ja teenusekokkulepped, lähtudes ülesannete lõplikust jaotusest ning õigusaktidest tulenevast pädevusest ja vastutusest. Kokkulepetes täpsustame poolte rollid ja ülesanded ning määrame kindlaks koostöö- ja teabevahetuse korra, sealhulgas selle, kuidas edastatakse asjaomasele IT-teenuse osutajale tema ülesannete täitmiseks vajalik teave andmekaitsealase mõjuhinnangu vajaduse hindamise tulemuste ning mõjuhinnangus tuvastatud riskide ja riskimaandamismeetmete kohta. Ümberkorralduse ettevalmistamisel ja üleminekuperioodil lähtume kehtivatest andmekaitsenõuetest ning tagame vajaliku teabevahetuse senise teenusekorralduse raames.
TRAM	**Kommentaar ettepaneku punktile 27**: Asutuses on mõjuhinnangute koostamise põhimõtted ja asjaomased rollid sätestatud kehtivas isikuandmete töötlemise korras. Protsessi toetavad mõjuhinnangute vormid ja nende täitmist abistavad juhendid. Korras on kirjeldatud mõjuhinnangu vajaduse hindamise ja koostamise põhinõuded ning protsess. Kuna asutuses vaadatakse korda töökorralduslikult vähemalt üks (1) kord aastas üle, on võimalik protsessikirjeldusi vajaduse korral ajakohastada ja täiendada. Leiame, et asutuses on mõjuhinnangute tegemiseks vajalik töökorralduslik raamistik olemas ning oleme valmis seda vajaduse korral täiendama, et tagada nõuete täitmine ja protsessi parem jälgitavus. **Kommentaar ettepaneku punktile 28**: TRAM-s on kehtestatud IT arendusprojektide kord. Vaatame kehtiva korra üle ning hindame vajadust täiendada seda DPIA vajaduse hindamise ja AKS-i kaasamise nõuetega, et tagada nende õigeaegne arvestamine IT arendusprojektide kavandamisel ja elluviimisel. **Kommentaar ettepanek TRAM-ile** (ettepaneku punkt 32): Asutusel on andmekogude põhimääruste kohaselt volitatud töötleja roll liiklusjärelevalve infosüsteemi ja sadamaregistri puhul, mille vastutav töötleja on KliM. Võtame ettepaneku arvesse, täpsustame ning vajadusel täiendame koostööpõhimõtteid ja töökorraldust, et tagada riskide hindamiseks ja andmekaitsealase mõjuhinnangu koostamiseks vajaliku teabe õigeaegne tuvastamine ja edastamine vastutavale töötlejale. Vaatame üle ülesannete ja vastutuse selge jaotuse ning asjakohaste toimingute dokumenteerimise. Hindame olemasolevaid põhimõtteid ning vajadust täiendada neid põhimõtteid ka uute andmekogude, infosüsteemide, süsteemiarenduste jms arenduste protsessi.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Reguleeritakse isikuandme kaitse korras, millise tähtajad ja vastutaja on toodud ülal.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	Nõus, et sellega tuleks tegeleda. Vastutatavatel töötlejatel palun edastada DPIA info ka KeMIT-ile. Hetkel me pole näinud veel ühegi KeMIT-i kriitilise andmekogu DPIA-d, kuigi tihti selle vajadus on ilmselge.

EGT	EGT toetab mõjuhinnangu vajaduse hindamise ja koostamise korralduse kirjeldamist ning ühise eelhinnangu vormi ja mõjuhinnangu näidise väljatöötamist. Geoloogiafondi puhul tuleb esmalt hinnata isikuandmete töötlemise olemasolu ja ulatust ning seejärel eraldi mõjuhinnangu vajadust. Isikuandmete esinemine ei pruugi tähendada iseenesest mõjuhinnangu kohustust.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud. AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

5. Välisveebis avaldatud privaatsusteave

Lähtekoht: Asutusel on selgelt määratletud vastutus ja toimiv praktika, mis tagab välisveebis avaldatud privaatsustingimuste ja isikuandmete töötlemise põhimõtete avaldamise, regulaarse ülevaatamise, ajakohastamise ning muudatuste õigeaegse kajastamise. Praktika hõlmab vastutava isiku või rolli määramist, ülevaatamise sageduse kujundamist ning ajakohaste andmete nähtavust asutuse veebilehel. Välisveebis avaldatud privaatsusteave peab sisaldama vähemalt GDPR artiklites 13–14 nõutud teavet.

JÄRELDUS 25 — välisveebis avaldatud privaatsusteabe olemasolu. KliM valitsemisala asutused on üldjuhul taganud välisveebis andmesubjektidele suunatud isikuandmete töötlemise teabe avaldamise. KliMil, TRAMil, KeAl, KAURil, RiLil, KeMITil ja ELMil on välisveebis avaldatud isikuandmete töötlemise põhimõtted, privaatsuspoliitika või muu samaväärne andmekaitseteave. **EGTs ei olnud 01.10.2026 seisuga välisveebis avaldatud isikuandmete kogumise ja töötlemise põhimõtteid** ning nende avaldamine on kavandatud pärast isikuandmete kaitsega seotud alusdokumentide valmimist. Kuna GDPRi artiklid 12–14 eeldavad, et andmesubjektile antakse isikuandmete töötlemise kohta selge, arusaadav ja kergesti kättesaadav teave, **ei ole EGT puhul töö ajal olnud andmesubjektidele tagatud samaväärne juurdepääs isikuandmete töötlemise teabele nagu teistes valitsemisala asutustes**.

JÄRELDUS 26 — privaatsusteabe ajakohastamise vastutus ja regulaarsus. Välisveebis avaldatud isikuandmete töötlemise põhimõtete ajakohasuse tagamise eest vastutab asutus kui vastutav töötleja. AKSi ülesanne on asutust nõustada ja jälgida isikuandmete kaitse nõuete täitmist. Sisemise töökorraldusega võib AKSile või andmekaitse töörühmale anda ka andmekaitsetingimuste koostamise, ajakohastamise ja ülevaatamise praktilisi ülesandeid, kui see ei kahjusta AKSi sõltumatust ega tekita huvide konflikti, kuid see ei vii vastutust asutuselt üle AKSile ega töörühmale.

Asutustes on välisveebis avaldatud isikuandmete töötlemise põhimõtete ajakohastamine praktikas üldjuhul seotud AKSi või andmekaitse töörühma rolliga, kuid organisatsioonisisene ülesannete jaotus, ülevaatamise sagedus ning muudatustest teavitamise ja ajakohastamise töökorraldus ei ole kõigis asutustes selgelt dokumenteeritud.

KliMis on andmekaitsetingimuste ajakohasuse kontrollimine ja vähemalt kord aastas ülevaatamine ette nähtud isikuandmete kaitse korra eelnõus ning AKS on tingimuste ülevaatamises ja korrigeerimises ka praktikas osalenud. TRAMis toimub tingimuste ajakohastamine koostöös sisuvaldkondadega AKSi eestvedamisel ning KeAs koondab andmekaitse töörühm sisendi, sõnastab ajakohastamise ettepanekud ja kontrollib tingimuste vastavust tegelikule töökorraldusele. TRAMis ja KeAs ei ole vastutus ega regulaarse ülevaatamise kord ametijuhendis, töörühma ülesannete kirjelduses või muus sisemises töökorralduses selgelt määratud. KAURis vaatab AKS andmekaitsetingimusi üle ja korraldab vajalike muudatuste edastamise veebihaldurile või -administraatorile, kuid regulaarset ülevaatamistsüklit ei ole kehtestatud ning ülevaatamine toimub vajaduspõhiselt. Ka RiLis ei ole kehtestatud regulaarset ülevaatamistsüklit ning ülevaatamine toimub vajaduspõhiselt. KeMITis on ajakohastamisega seotud ülesannete jaotus ja iga-aastane ülevaatamine selgemalt korraldatud ning AKS hindab kord aastas välisveebis avaldatud põhimõtete ajakohasust ja edastab vajadusel sisuhaldurile uuendatud versiooni.

GDPR ei nõua kindla ülevaatamissageduse kehtestamist ning regulaarse tsükli puudumine ei tähenda iseenesest, et andmekaitsetingimused ei ole ajakohased. Asutuse sisemises töökorralduses selle selge määratlemine, kes ja kuidas jälgib andmekaitsetingimusi mõjutavaid muudatusi, edastab vajaliku teabe ning korraldab tingimuste ajakohastamise, aitaks vähendada riski, et välisveebis avaldatud teave ei kajasta õigel ajal õigusaktide, tööprotsesside, infosüsteemide või kontaktkanalite muutumist.

JÄRELDUS 27 — andmekaitseküsimuste kontaktkanalite olemasolu ja toimivus. Mitmes asutuses ilmnes puudusi andmekaitseküsimuste kontaktkanalite olemasolus, avalikustatud kontaktandmete õigsuses või kontaktkanali tehnilises toimivuses. RiLi välisveebi privaatsussätete rubriik ei sisaldanud 08.01.2026 seisuga

kontaktkanalit isikuandmete töötlemisega seotud küsimuste, päringute ja taotluste esitamiseks, kuid see lisati töö käigus. ELMi privaatsuspoliitika rubriik ei sisaldanud 01.10.2026 seisuga teavet kontaktkanali kohta, mille kaudu andmesubjekt saaks pöörduda asutuse poole isikuandmete töötlemisega seotud küsimustes või oma õiguste kasutamiseks. KeAs tuvastati töö käigus ebaõige kontaktandmete viide ning KeMITis ei toiminud välisveebil avaldatud kontaktkanal nõuetekohaselt; mõlemad probleemid lahendati töö käigus. **EGTs ei olnud 01.10.2026 seisuga välisveebis avaldatud kontaktkanalit. Aruande kommentaarimise ajal lisati välisveebilehele AKSi kontaktandmed, kelle poole saab kodanik pöörduda EGTs toimuva isikuandmete töötlemise ja andmesubjekti õiguste kasutamise küsimustes.** Asjakohase, õige ja toimiva kontaktkanali puudumine võib raskendada andmesubjektil asutusega suhtlemist ning takistada või viivitada isikuandmete kaitse üldmääruse artiklites 15–22 sätestatud õiguste kasutamist, sh õigust tutvuda andmetega, nõuda andmete parandamist või kustutamist, piirata andmete töötlemist, saada andmeid üle kantavas vormis, esitada töötlemisele vastuväiteid ning kasutada automatiseeritud töötlusel põhinevate üksikotsustega seotud õigusi. Samuti võib kontaktkanali puudumine, ebatäpsus või mittetoimimine raskendada asutusel isikuandmete kaitse üldmääruse artiklis 12 sätestatud läbipaistva teavitamise ja andmesubjekti õiguste kasutamise hõlbustamise kohustuse ning artiklites 13 ja 14 sätestatud teavitamiskohustuste nõuetekohast täitmist.

JÄRELDUS 28 — privaatsusteabe sisuline täielikkus ja kooskõla tegeliku töökorraldusega. Välisveebis avaldatud privaatsusteave peab põhinema ajakohasel töötlemisülevaatel ja tegelikel teenuseprotsessidel ning kajastama andmesubjekti jaoks arusaadavalt töötlemise eesmärke, õiguslikke aluseid, õigusi, säilitustähtaegu, vastuvõtjate kategooriaid ja kontaktkanaleid. Töö käigus ilmnes, et osa asutusi on teavet hiljuti uuendanud või uuendamas: KliM kontrollis ja korrigeeris andmekaitsetingimusi 2025. aasta lõpus, TRAM tegi põhjalikuma uuenduse 24.11.2025, KAUR uuendas põhimõtteid 15.04.2026 ning RiL avaldas uuendatud põhimõtted 09.03.2026, kuid tuvastas hiljem täiendamisvajaduse. See näitab, et privaatsusteavet ajakohastatakse, kuid selle sisuline täielikkus sõltub sellest, kas veebis avaldatud teave on seotud tegelike töötlemistoimingute ja teenuseprotsessidega. Kui avaldatud teave ei vasta tegelikule töökorraldusele, võib see vähendada andmesubjekti võimalust mõista oma andmete töötlemist ning nõrgendada asutuse suutlikkust tõendada läbipaistvuse põhimõtte täitmist.

ETTEPANEK kõikidele asutustele:

33. Siduda välisveebis avaldatud andmekaitsetingimuste ajakohastamine asutuse isikuandmete töötlemistoimingute ülevaatamise ja muudatuste juhtimise protsessiga ning määrata selleks vastutavad rollid. Töötlemistoimingute ülevaatamise käigus ning oluliste muudatuste korral hinnata, kas välisveebis avaldatud teave on ajakohane, täielik, kooskõlas tegelike töötlemistoimingutega ning sisaldab toimivaid kontaktandmeid. Vajalikud muudatused teha põhjendamatu viivituseta ning ülevaatamise ja ajakohastamise tulemused dokumenteerida. Kuigi GDPR selleks ei kohusta, tasuks tingimuste ajakohasus kord aastas siiski üle vaadata. KeMITi ülesannete üleminekul Riigi Digikeskusesse, RIAsse ja KliMi tuleb teenindatavatel asutustel vajaduse korral hinnata, kas nende välisveebis avaldatud privaatsusteave ja kontaktandmed vajavad teenuseosutaja või andmekaitsealase infovahetuse muutumise tõttu ajakohastamist.

ETTEPANEK EGTle:

34. **Töötada välja ja avaldada EGT välisveebis asutuse tegelikest isikuandmete töötlemise protsessidest lähtuvad isikuandmete töötlemise põhimõtted**. Teave peab olema esitatud selges, arusaadavas ja kergesti leitavas vormis ning sisaldama vähemalt GDPRi artiklites 13–14 nõutud teavet, sh töötlemise eesmärke ja õiguslikke aluseid, andmesubjektide õigusi, säilitustähtaegu või nende määramise kriteeriume, vastuvõtjate kategooriaid, andmete edastamist puudutavat teavet, kui see on asjakohane, ning kontaktkanalit isikuandmete kaitsega seotud küsimuste esitamiseks. Kui ajutise lahendusena kasutatakse KliMi või mõne muu asutuse põhimõtteid, tuleb need enne avaldamist kohandada EGT tegelikele töötlemisprotsessidele, et avaldatav teave ei oleks andmesubjektide jaoks eksitav.

ETTEPANEK ELMile:

35. **Kui AKS on määratud, tuleb avaldada AKSi kontaktandmed või selgelt kirjeldatud kontaktkanal AKSiga ühenduse võtmiseks**. Täiendada välisveebis avaldatud privaatsuspoliitikat selgelt leitava kontaktkanaliga, mille kaudu andmesubjektid saavad esitada isikuandmete töötlemisega seotud päringuid, taotlusi ja õiguste kasutamise soove. Kontaktkanali nimetus ja kirjeldus peaksid olema andmesubjektile arusaadavad ning selgelt seostatavad isikuandmete kaitse küsimustega. Samuti tuleks määrata vastutaja ja ajakava privaatsuspoliitika regulaarseks ülevaatamiseks ning ajakohastamiseks.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*
KliM	Plaanis on üle vaadata ja ajakohastada KliMi välisveebi privaatsusteavitus. Samuti on eesmärk siduda privaatsusteavituse ajakohastamine töötlemistoimingute ülevaatamise ja muudatuste juhtimise

	protsessiga, et isikuandmete töötlemises toimuvad muudatused kajastuksid vajaduse korral õigeaegselt privaatsusteavituses.
TRAM	**Kommentaar ettepanek TRAM-ile** (ettepaneku punkt 33): Asutus ei pea otstarbekaks siduda välisveebis avaldatud andmekaitsetingimuste ajakohastamist vahetult töötlemistoimingute ülevaatamise ja muudatuste juhtimise protsessiga ega kehtestada selleks täiendavaid kohustuslikke tähtaegu ja vastutusahelaid, arvestades töötlemistoimingute rohkust ja järjepidevust. Välisveebi ülevaatamist korraldab asutuses kommunikatsiooniosakond, kes teavitab struktuuriüksuste juhte veebis avaldatud info ülevaatamise vajadusest üks (1) korda aastas. Sellekohase teavituse ja tagasiside küsimise saadab AKS samuti samal ajal teenusejuhtidele isikuandmete töötlemise osas. Töötlemisülevaate osas aga ei näe me vajadust neid igal aastal kohustuslikus korras üle vaadata, kui muudatusi ei ole toimunud.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Võtame soovituse teadmiseks ja kaalume selle rakendamist (GDPR ei nõua kindla ülevaatamissageduse kehtestamist).
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	Nõus. Meie vaates tegemist pideva tööga, millega tuleb tegeleda.
EGT	EGT nõustub vajadusega avaldada välisveebis tegelikest töötlemistoimingutest lähtuvad isikuandmete töötlemise põhimõtted ning selgelt leitavad andmekaitseküsimuste kontaktandmed. Üldiste põhimõtete kohandamisel tuleb arvestada EGT tööprotsessidega.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud. AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

6. Isikuandmetega seotud rikkumiste käsitlemine

Lähtekoht: Asutustes on kehtestatud ja rakendatud GDPRi nõuetele vastav isikuandmetega seotud rikkumiste käsitlemise korraldus, mis tagab rikkumiste õigeaegse tuvastamise, riskipõhise hindamise, dokumenteerimise, lahendamise ning vajaduse korral AKI ja andmesubjektide teavitamise. Korralduses on määratud vastutava ja volitatud töötleja ülesanded, vastutus, teabevahetus ning rikkumise eskaleerimise ja teavitamise kord. Korralduse järgimine ja toimivus on praktikas tõendatav.

JÄRELDUS 29 — isikuandmetega seotud rikkumiste käsitlemise miinimumpraktika ning asutusesiseste kordade ja juhiste piisavus. GDPRi artiklite 33 ja 34 kohaselt **peab vastutav töötleja dokumenteerima isikuandmetega seotud rikkumised**, hindama nendega kaasnevat ohtu füüsiliste isikute õigustele ja vabadustele ning teavitama nõutavatel juhtudel põhjendamatu viivituseta Andmekaitse Inspektsiooni ja andmesubjekti. AKIt

tuleb põhjendamatu viivituseta ja võimaluse korral teavitada 72 tunni jooksul pärast rikkumisest teada saamist ning kui teavitamine toimub hiljem, tuleb viivitust põhjendada.

KliM valitsemisalas on isikuandmetega seotud rikkumiste käsitlemine korraldatud asutuste lõikes erineva põhjalikkusega. Mõnes asutuses on vastavad põhimõtted kehtestatud, mõnes osaliselt kirjeldatud ning mõnes alles väljatöötamisel või terviklikult kehtestamata. Kuigi GDPR ei nõua kõigis asutustes vormilt ja sisult identset menetluskorda ega eraldiseisva dokumendi kehtestamist, peab iga asutus tagama toimiva, terviklikult jälgitava ja teenistujatele kättesaadava miinimumkorralduse. See peab hõlmama võimaliku rikkumise tuvastamist, asutusesisest teatamist ja eskaleerimist, menetluses osalevate isikute rollide ja vastutuse määramist, rikkumise asjaolude ja võimalike tagajärgede väljaselgitamist, füüsiliste isikute õigustele ja vabadustele avalduva ohu hindamist, AKI ja andmesubjekti teavitamise otsustuskriteeriume ja tähtaegu ning menetluse terviklikku ja kontrollitavat dokumenteerimist. GDPRi artikli 33 lõike 5 kohaselt peab dokumentatsioon kajastama vähemalt rikkumise asjaolusid, mõju ja võetud parandusmeetmeid viisil, mis võimaldab järelevalveasutusel nõuete täitmist kontrollida. Lisaks peaks menetluse dokumentatsioon sisaldama riskihinnangut, teavitamise või teavitamata jätmise otsust ja selle põhjendust, rakendatud mõju leevendavaid ja ennetavaid meetmeid ning menetluse lõpetamise aega. Protsess võib olla kirjeldatud ühes korras või mitmes omavahel seostatud korras ja juhises, kui nende põhjal on menetluskäik tervikuna arusaadav ja jälgitav.

TRAMis ja KeMITis on isikuandmetega seotud rikkumiste käsitlemine kirjeldatud kehtivates kordades. TRAMis vajasid täpsustamist eelkõige rikkumise tuvastamise, selle mõju hindamise, AKI või andmesubjekti teavitamise üle otsustamise ning menetluskäigu dokumenteerimise põhimõtted. Samuti ei olnud korras sätestatud volitatud töötleja teavitamis- ja tegutsemiskohustusi isikuandmetega seotud rikkumise avastamisel. Nimetatud puudused on 03.09.2026 ajakohastatud isikuandmete töötlemise korras kõrvaldatud. KeMITi puhul tuleb eristada tema tegevust vastutava ja volitatud töötlejana, sest rollist sõltub, kes teeb AKI või andmesubjekti teavitamise otsuse ja kellele tuleb vajalik teave edastada. KeMITi teenindatavatele asutustele on KeMITi osutatava IT-teenusega seotud intsidentidest, sh andmekaitseintsidentidest, teatamine ja nende haldamine reguleeritud, kuid täpsustamist vajavad teenindatavas asutuses pärast teate saamist tehtavad toimingud ning selliste isikuandmetega seotud rikkumiste käsitlemine, mis ei ole seotud KeMITi osutatava IT-teenusega. KeMITi korrad ja juhised ei anna teenindatavatele asutustele terviklikku ülevaadet RITi vastutusalasse kuuluvate juhtumite käsitlemisest.

KliMis ja KeAs on täpsemad põhimõtted kavandatud koostamisel olevates isikuandmete kaitse kordades, kuid töö läbiviimise ajal ei olnud need veel kehtestatud ning menetlus sõltub seni olemasolevatest teavitamise ja asjaajamise põhimõtetest, AKSi või andmekaitse töörühma kaasamisest ning kujunenud praktikast.

KAURis on isikuandmetega seotud rikkumise käsitlemise eri etapid kirjeldatud KAURi siseveebi isikuandmete kaitse teemalehel, teabehalduse korras ja selle lisades ning KeMITi materjalides. Kirjeldatud on mh võimalikust rikkumisest teavitamine, teavituse registreerimine ja edastamine ning AKSi kaasamine. Kuigi AKSi sõnul on menetlus praktikas toimiv, ei ole kogu menetluskäik rikkumise asjaolude ja mõju hindamisest kuni AKI või andmesubjekti teavitamise otsustamise, selle põhjendamise ja dokumenteerimiseni esitatud ühes terviklikult jälgitavas protsessikirjelduses ning tervikpildi saamiseks tuleb eri allikates paiknev teave omavahel seostada.

RiLis kasutatakse üldist mittevastavuste menetlemise korda, mis ei käsitle eraldi GDPRi artiklitest 33 ja 34 tulenevaid isikuandmetega seotud rikkumise hindamise ja teavitamise küsimusi.

EGTs ja ELMis puudus töö ajal terviklik isikuandmetega seotud rikkumiste käsitlemise korraldus. EGT puhul tuleb sellise korralduse väljatöötamisel arvestada ka ajalooliste andmestikega, mille isikuandmete koosseis, ulatus, säilitamise põhjendatus ja juurdepääsud võivad mõjutada võimaliku rikkumise mõju hindamist. ELMis ei nähtu kogutud teabe põhjal selgelt roll või isik, kes korraldab isikuandmetega seotud rikkumise hindamise, otsustab edasised tegevused ning tagab teavitamise ja dokumenteerimise.

Seega ei ole puudus kõigis asutustes sama laadi: osal asutustel on vaja olemasolevaid kordi või juhiseid täpsustada ja omavahel selgemalt seostada, osal pooleliolevad korrad kehtestada ning osal kirjeldada isikuandmetega seotud rikkumiste käsitlemise protsess tervikuna. Ühtse miinimumpraktika puudumine suurendab riski, et sisult sarnaseid juhtumeid hinnatakse ja menetletakse valitsemisala asutustes erinevalt. Ühes asutuses võidakse juhtum eskaleerida võimaliku isikuandmetega seotud rikkumisena, samal ajal kui teises käsitatakse seda üksnes IT- või töökorraldusliku intsidendina. Selle tulemusena võib rikkumise õiguslik tähendus jääda õigel ajal tuvastamata, oht füüsiliste isikute õigustele ja vabadustele piisavalt hindamata ning AKI või andmesubjekti teavitamise vajadus nõuetekohaselt ja dokumenteeritult otsustamata.

KeMITi ümberkorraldamisel ning tema ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliMi vahel tuleb hinnata, millised KeMITi tegevuse lõppemisel kehtivuse kaotavates kordades või juhistes reguleeritud isikuandmetega seotud rikkumiste käsitlemise põhimõtted tuleb üle võtta asjaomaste valitsemisala asutuste kordadesse või juhistesse ning millised küsimused tuleb reguleerida uues teenusekorralduses koostöös asjaomase teenuseosutajaga.

JÄRELDUS 30 — tehnilise intsidendihalduse ja andmekaitsealase otsustuse eristamine. KliM valitsemisalas toetavad tehniliste intsidentide käsitlemist KeMITi ja RITi intsidendihalduse protsessid, mis hõlmavad intsidendi tuvastamist ja registreerimist, esmast analüüsi, logide ja ajatelje koondamist, eskaleerimist, tehnilist lahendamist ning dokumenteerimist. Need protsessid loovad olulise aluse isikuandmetega seotud rikkumise asjaolude väljaselgitamiseks, kuid ei asenda asutuse kui vastutava töötleja kohustust hinnata, kas konkreetne juhtum on GDPRi artikli 4 punkti 12 tähenduses isikuandmetega seotud rikkumine ning kas tekib GDPRi artiklite 33 ja 34 kohane AKI või andmesubjekti teavitamise kohustus.

Isikuandmeid mõjutava või mõjutada võiva juhtumi korral näevad nii KeMITi kui ka RITi korrad ette asjaomase asutuse AKSi kaasamise ning hindamiseks vajaliku tehnilise teabe koondamise ja edastamise. KeMITi kehtivas korras on sätestatud ka kaasamise tähtajad.

Iga asutus peab vastutava töötlejana määrama oma töökorralduses rolli või üksuse, kes korraldab isikuandmetega seotud rikkumise hindamise ja teavitamisotsuse tegemise. AKS tuleb hindamisse kaasata kooskõlas tema GDPRist tulenevate ülesannetega. IT-teenuse osutaja peab koostöös teenindatava asutusega tagama, et hindamiseks vajalik tehniline teave jõuab vastutava töötleja määratud rolli või üksuseni põhjendamatu viivituseta ja piisava ajavaruga GDPRi artiklites 33 ja 34 sätestatud kohustuste täitmiseks. Kui IT-teenuse osutaja tegutseb volitatud töötlejana, peab ta GDPRi artikli 33 lõike 2 kohaselt teatama isikuandmetega seotud rikkumisest vastutavale töötlejale põhjendamatu viivituseta. **KeMITi ümberkorraldamisel ning tema ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliMi vahel tuleb teenindatavatel asutustel ja asjaomastel IT-teenuse osutajatel koostöös tagada, et tehniliste intsidentide ja võimalike isikuandmetega seotud rikkumiste käsitlemise vastutus, teabevahetus, kontaktpunktid, kaasatavad osalised ning kaasamise tähtajad oleksid ka uues teenusekorralduses selgelt määratud. IT-teenuse osutaja määrab enda intsidendihalduse protsessid ise, kuid teenindatavate asutustega tuleb kokku leppida pooltevaheline tööjaotus ja teabevahetus viisil, mis võimaldab vastutaval töötlejal täita GDPRi artiklitest 33 ja 34 tulenevaid kohustusi.**

JÄRELDUS 31 — vastutava ja volitatud töötleja rollid ja infovahetus isikuandmetega seotud rikkumiste käsitlemisel. Asutustes, mille tehnilist intsidendihaldust või infosüsteemide haldust toetab KeMIT või RIT, on oluline, et volitatud töötleja edastaks vastutavale töötlejale rikkumise hindamiseks vajaliku teabe piisava detailsuse ja kiirusega. Positiivse näitena on KliMi ja RITi andmetöötluslepingus sätestatud volitatud töötleja kohustus teavitada vastutavat töötlejat isikuandmetega seotud rikkumisest või selle kahtlusest põhjendamatu viivituseta ning edastada hiljemalt 24 tunni jooksul teadaolev teave, mis on vajalik järelevalveasutuse teavitamise kohustuse hindamiseks ja täitmiseks. Samas ilmnes KliMis ebaselgus selles, kas ja millistel juhtudel jõuab intsidendihalduse kanali kaudu esitatud info AKSini. Kui infovahetuse tähtajad, teabe koosseis ja AKSi kaasamise põhimõtted ei ole selgelt kokku lepitud, võib suureneda risk, et rikkumise hindamine ja teavitamise otsus viibib. Volitatud töötleja roll on anda vastutavale töötlejale õigeaegselt piisav teave rikkumise hindamiseks; AKI või andmesubjekti teavitamise otsus ja vastutus jäävad vastutavale töötlejale. Pooled võivad kokku leppida praktilise tööjaotuse teavituse ettevalmistamisel või edastamisel, kuid see ei muuda vastutava töötleja vastutust GDPRi artiklite 33 ja 34 nõuete täitmise eest.

JÄRELDUS 32 — teenistujate teadlikkus rikkumiste tuvastamisel ja teavitamisel. KliM valitsemisalas on avaldatud juhised isikuandmetega seotud rikkumiste tuvastamiseks ja neist teavitamiseks ning teavitamiskohustust on käsitletud infoturbekoolitustel. Juhised asuvad praegu ligipääsetavas varasemas haldusala siseveebis, mille materjale enam ei ajakohastata ja mis suletakse kavakohaselt pärast kõigi asutuste üleminekut ATK 2.0 arvutitöökoha teenusele, eeldatavasti 2026. aasta lõpuks. Koolituste kohta kogutud teabe kohaselt on mitmes asutuses isikuandmete kaitse koolitusi korraldatud harva või vajaduspõhiselt või ei ole neid ülevaateperioodil toimunud. Ajakohastamata juhendmaterjalid ja koolituste ebaregulaarne korraldamine suurendavad riski, et teenistuja ei tuvasta juhtumi võimalikku seost isikuandmetega või ei märgi seda IT-teenust osutavale asutusele edastatud rikkumisteates. See võib takistada rikkumise nõuetekohast kvalifitseerimist ja AKSile edastamist ning põhjustada viivitusi rikkumise ulatuse hindamisel, maandamismeetmete rakendamisel ja vajaduse korral AKI või andmesubjektide teavitamisel.

ETTEPANEK KliMile koostöös valitsemisala asutuste AKSidega:

36. Koostada asutustes isikuandmetega seotud rikkumiste käsitlemise miinimumprotsessi toetamiseks soovituslik juhis või näidisprotsess, milles kirjeldatakse õigusaktidest tulenevaid miinimumnõudeid ja antakse suunised nende rakendamiseks, ning lisada see valmivale valitsemisalaülesele siseveebilehele. Juhis või näidisprotsess peaks käsitlema vähemalt rikkumise tuvastamist, asjaomaste rollide kaasamist, füüsiliste isikute õigustele ja vabadustele avalduva ohu hindamist, AKI ja andmesubjekti teavitamise üle otsustamist ning menetluskäigu ja tehtud otsuste dokumenteerimist. Asutused saavad juhist või näidisprotsessi kohandada oma töökorralduse, riskiprofiili, infosüsteemide ja kasutatavate teenusepakkujate järgi. Juhise koostamisel arvestada, et IT-teenuse osutaja määrab enda sisemised intsidendihalduse protsessid ise, kuid asutuse ja IT-teenuse osutaja vaheline tööjaotus ning teabevahetus peavad võimaldama asutusel täita vastutava töötleja kohustusi.

ETTEPANEK kõikidele asutustele:

37. Tagada, et asutuses oleks dokumenteeritud ja teenistujatele kättesaadav isikuandmetega seotud rikkumiste käsitlemise miinimumprotsess alates rikkumise avastamisest kuni menetluse lõpetamiseni. Protsess peaks hõlmama vähemalt rikkumise tuvastamist, esmase teavituse kanalit, AKSi kaasamist, rollide ja vastutuse jaotust, rikkumise asjaolude ning mõju ja riskitaseme hindamist, AKI ja vajaduse korral andmesubjekti teavitamise otsustuskriteeriume, 72 tunni tähtaja arvestamist, menetluskäigu dokumenteerimist ning parandusmeetmete rakendamist ja jälgimist. Protsess võib olla kirjeldatud isikuandmete kaitse korras, infoturbe või intsidendihalduse korras, mittevastavuste menetlemise korras, siseveebi juhises või mitmes omavahel seotud dokumendis, kuid nende põhjal peab kogu menetluskäik olema tervikuna teenistujatele kättesaadav ja jälgitav ning praktikas rakendatav. Selleks:
    - KliMil ja KeAl ajakohastada koostamisel olevates isikuandmete kaitse kordades RITi ja KeMITi ülesannete vastutuse ja teabevahetuse kirjeldust lähtuvalt uuest teenusekorraldusest,
    - RiLil täiendada mittevastavuste menetlemise korda GDPRi artiklitest 33 ja 34 tulenevate isikuandmetega seotud rikkumiste hindamise, teavitamise ja dokumenteerimise erisustega;
    - EGTl ja ELMil määrata rollid, vastutus, otsustuskriteeriumid ja dokumenteerimisnõuded.
    - KAURil soovitame hinnata, kas olemasolev siseveebi juhis ja teised kohaldatavad korrad käsitlevad omavahel seostatuna kogu menetlusprotsessi, ning täiendada olemasolevat korraldust üksnes tuvastatud konkreetsete lünkade ulatuses.

KeMITi ümberkorraldamisel ning tema ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliMi vahel tuleb KliMil ja teenindatavatel asutustel koostöös asjaomaste IT-teenuse osutajatega hinnata, millised KeMITi tegevuse lõppemisel kehtivuse kaotavates kordades ja juhistes sätestatud rikkumiste käsitlemise põhimõtted tuleb kajastada asutuste kordades või juhistes ning millised küsimused tuleb reguleerida uues teenusekorralduses. Seejuures tuleb tagada, et vastutus, teabevahetus, kontaktpunktid, kaasatavad osalised ja kaasamise tähtajad oleksid asutuste sisemistes dokumentides ning teenuse- ja koostöökokkulepetes omavahel kooskõlas ja selgelt kirjeldatud.

ETTEPANEK KeMITi või RITi teenuseid kasutavatele valitsemisala asutustele koostöös asjaomase IT-teenuse osutajaga:

38. IT-teenuse osutamise ja andmetöötluskokkulepete sõlmimisel või muutmisel seada eesmärgiks, et kokkulepped sisaldaksid teavet selle kohta, millist teavet, millise tähtaja jooksul ja millise kanali kaudu edastab volitatud töötleja vastutavale töötlejale isikuandmetega seotud rikkumise või selle kahtluse korral. Kokkulepetes tuleks käsitleda vähemalt teavitamise tähtaega, minimaalselt edastatavat teavet, logide ja ajatelje kättesaadavust, AKSi kaasamise korda, tehniliste meetmete rakendamist ning vastutava töötleja otsustusõiguse ja vastutuse säilimist AKI ja andmesubjektide teavitamise üle otsustamisel. Samuti tuleks kirjeldada volitatud töötleja kogutud tehnilise teabe, tehtud tegevuste ja edastatud teavituste dokumenteerimist. KeMITi ülesannete jaotamisel Riigi Digikeskuse, RIA ja KliMi vahel ning RITi ühendamisel RIAga tuleb KliMil ja teenindatavatel asutustel koostöös asjaomaste IT-teenuse osutajatega seada eesmärgiks, et uues teenusekorralduses oleksid samasisuline infovahetus, tehnilise teabe kättesaadavus, kontaktpunktid ja teenindatavate asutuste AKSide kaasamine selgelt kokku lepitud.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*
KliM	Üldiselt nõustume ettepanekuga koostada rikkumisjuhtumite lahendamiseks valitsemisalaülene praktiline juhis. Samas ka nõustume, et juhise koostamisel tuleb arvestada asutuste erineva töökorralduse, struktuuri ja rollijaotusega. Hetkel on KliMil endal asutusesisene Excel IT teenustega mitteseotud rikkumisjuhtumite registreerimiseks, kuid selle lahenduse vaatame üle. Juhise rakendamise kõrval on oluline ka töötajate teadlikkuse tõstmine, et rikkumisjuhtumitest osataks õigel ajal ja õigetele isikutele teada anda. Samuti on plaanis üle vaadata rikkumisjuhtumitega seotud infovahetuse korraldus IT-teenuste osutajatega, arvestades eesootavaid muudatusi IT-teenuste korralduses. Seda on mõistlik teha siis, kui muudatuste täpsem sisu ja sellest tulenev töökorraldus on selgunud. Juhime tähelepanu, et järelduses 32 märgitud juhised on lisaks haldusala siseveebile kättesaadavad ka KLIMi enda siseveebis, mida uuendatakse regulaarselt. **Nõustume ettepanekutega 37 ja 38.** Jätkame KeMITi ülesannete ümberkorraldamise raames Riigi Digikeskuse ja RIAga arutelusid isikuandmetega seotud rikkumiste käsitlemise korralduse üle. Hindame, millised KeMITi senistes kordades ja juhistes sätestatud põhimõtted tuleb kajastada asutuste sisemistes dokumentides ning millised küsimused reguleerida teenuse- ja koostöökokkulepetes. Ümberkorraldamise käigus ajakohastame oma sisemised dokumendid ning sõlmime vajalikud kokkulepped või muudame olemasolevaid. Kirjeldame neis selgelt ja omavahel

	kooskõlas poolte ülesanded ja vastutuse, kontaktpunktid ning koostöö- ja teabevahetuse korra, sealhulgas AKSide ja teiste osaliste kaasamise tähtajad. Riigi Digikeskuse ja RIA kui volitatud töötlejatega täpsustame rikkumisest või selle kahtlusest teavitamise tähtajad, kanalid ja edastatava teabe, logide ja sündmuste ajatelje kättesaadavuse, tehniliste meetmete rakendamise ning tegevuste ja teavituste dokumenteerimise. KliMile kui vastutavale töötlejale jääb vastutus AKI ja andmesubjektide teavitamise vajaduse hindamise ning teavitamiskohustuste täitmise eest. Koostöös teenuseosutajatega tagame rikkumiste käsitlemise järjepidevuse ka üleminekuperioodil.
TRAM	**Täpsustus järelduse punktile 29**: Asutuses on 03.09.2026 kinnitatud isikuandmete töötlemise korras täpsustatud isikuandmetega seotud rikkumistest teavitamise ja rikkumiste menetlemise korda ning määratletud asjaomased rollid ja vastutusalad. Seega on järelduses nimetatud valdkond kehtivas korras reguleeritud.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Hindame, kas olemasolev siseveebi juhis ja teised kohaldatavad korrad käsitlevad omavahel seostatuna kogu menetlusprotsessi, ning vajadusel täiendame olemasolevat korraldust. RITiga lepingu sõlmimisel võetakse arvesse punktis 38 nimetatut. Tähtajad ja vastutaja on nimetatud ülal.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	Nõus ettepanekutega – oleme valmis koostööks Kliimaministeeriumi ja selle valitsemisalaga.
EGT	EGT nõustub rikkumiste käsitlemise korralduse täpsustamise vajadusega ning toetab ühise näidisprotsessi koostamist. AKS võib nõustada, osaleda asjaolude ja riskide hindamises ning koordineerida menetlustoiminguid. Teavitamisotsuse ja parandusmeetmete üle otsustamise pädevus peab olema asutuses eraldi määratud, vastutava töötleja vastutus jääb EGT-le, otsuseid teeb juhtkond.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud. AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.

7. Volitatud töötlejad ja lepingud

Lähtekoht: Asutus on kehtestanud ja rakendab ühtset korda volitatud töötlejate valikuks, kaasamiseks ja järelevalveks. Enne kaasamist hinnatakse ja dokumenteeritakse volitatud töötleja suutlikkus tagada isikuandmete töötlemise vastavus GDPRile ning asjaomaste hangete ja lepingute kooskõlastamisse kaasatakse AKS või muu määratud vastutaja. Volitatud töötleja kaasamine põhineb GDPRi artikli 28 nõuetele vastaval lepingul või muul siduval õigusaktil, milles määratakse kindlaks töötlemise tingimused, poolte õigused ja kohustused, turvameetmed, vastutava töötleja abistamine, nõuete täitmise tõendamine, auditeerimise võimalus ning andmete tagastamine või kustutamine. Teiste volitatud töötlejate kaasamine toimub dokumenteeritult ja vastutava töötleja eelneval kirjalikul loal, tagades üldise loa korral muudatustest teavitamise ja

vastuväidete esitamise võimaluse. Volitatud töötlejate nõuete täitmise üle tehakse regulaarset riskipõhist järelevalvet ning kontrollide tulemused, puudused ja parandusmeetmed dokumenteeritakse.

JÄRELDUS 33 — AKSi kaasamine hangete ja lepingute ettevalmistamisse. GDPRi artikli 38 lõike 1 kohaselt tuleb AKS nõuetekohaselt ja õigeaegselt kaasata kõikidesse isikuandmete kaitsega seotud küsimustesse. Varane kaasamine on oluline eelkõige juhul, kui hanke, lepingu, teenuse, infosüsteemi, programmi, andmekogu või uue tööprotsessiga võib kaasneda isikuandmete töötlemine või volitatud töötleja kasutamine. AKS saab hinnata kavandatava andmetöötluse õiguspärasust ja sellega seotud isikuandmete kaitse riske, nõustada poolte andmetöötlusrollide ja vastutuse määramisel ning juhtida tähelepanu vajadusele käsitleda hanke- ja lepingudokumentides turvameetmeid, konfidentsiaalsust, alamtöötlejate kasutamist ja muid GDPRist, sh artiklist 28 tulenevaid nõudeid. **AKSi kaasamine ei vähenda vastutava töötleja ega vastava protsessi eest vastutavate isikute vastutust. Otsused lepingu sõlmimise, kavandatava töötlemislahenduse kasutamise ja sellega seotud riskide aktsepteerimise kohta peavad jääma selleks volitatud isikule või asutuse juhtimistasandile.**

KliM valitsemisala asutustes on AKSi kaasamine hangete, lepingute ja uute andmetöötlustoimingute kavandamisse korraldatud erinevalt. Erinevused võivad olla põhjendatud asutuste suuruse, ülesannete ja töökorralduse, hangete mahu ning isikuandmete töötlemise ulatuse ja riskitasemega. Seega ei pea kaasamise korraldus olema kõikides asutustes ühetaoline. Mitmes asutuses ei ole siiski piisavalt selgelt kindlaks määratud, millistel juhtudel tuleb AKS kaasata, millist nõu või hinnangut temalt oodatakse, kuidas tema esitatud seisukohti arvesse võetakse ning kelle pädevuses on nende põhjal otsuste tegemine ja riskide aktsepteerimine.

KliMis, KeAs, KAURis ja EGTs toetab AKSi kaasamist tema ülesannete seos õigusnõustamise või hangete ja lepingute kooskõlastamisega. Hankekordades ei ole siiski alati eraldi sätestatud andmekaitsealast kontrollikohta juhtudeks, kui hanke või lepingu esemega kaasneb isikuandmete töötlemine.

TRAMis, RiLis ja KeMITis kaasatakse AKS peamiselt vajaduse või hinnatud riski alusel.

Ebaühtlane ja osaliselt reguleerimata kaasamispraktika suurendab riski, et võrreldava andmekaitseriskiga juhtumeid käsitletakse valitsemisala asutustes erinevalt ning andmekaitsenõudeid ei võeta hanke-, lepingu- või projektiprotsessis arvesse piisavalt vara.

JÄRELDUS 34 — volitatud töötleja tingimuste kajastamine lepingutes. Juhtudel, kus lepingupartner töötleb isikuandmeid asutuse nimel, tuleb GDPRi artikli 28 kohased tingimused üldjuhul sätestada lepingus või selle lisas. Muu siduv õigusakt saab olla aluseks üksnes juhul, kui see reguleerib konkreetset töötlemissuhet piisava detailsusega.

Töö käigus vaadeldi valitud lepinguid ja lepingumalle eesmärgiga mõista, kuidas on lepingutes arvestatud võimaliku isikuandmete töötlemise ja volitatud töötleja tingimustega. Vaatlus ei hõlmanud iga lepingu sisulist analüüsi ulatuses, mis võimaldaks kõigil juhtudel kindlaks teha, kas konkreetse lepingu täitmisel tegelikult töödeldi isikuandmeid asutuse nimel või kas lepingupartner tegutses volitatud töötlejana. Seetõttu ei saa üksnes asjaolust, et vaadeldud lepingutes või lepingumallides ei olnud eraldi või terviklikke andmetöötlustingimusi sätestatud, järeldada, et konkreetne leping oleks olnud GDPRi artikli 28 nõuetega vastuolus.

KliM valitsemisala asutustes kasutatakse hanke- ja lepingumenetluse lihtsustamiseks tüüplepinguid ja üldtingimusi. Vaadeldud dokumentidest ilmnes, et andmekaitsetingimusi käsitletakse lepingutes erineva detailsusega.

KliMi üldtingimustes ei olnud eraldi volitatud töötleja tüüptingimusi kirjeldatud. AKSi selgituse kohaselt vormistatakse isikuandmete töötlemise tingimused vajaduse korral eraldi andmetöötluslepinguna või põhilepingu lisana. Kui isikuandmete töötlemise vajadus nähtub lepingu kavandist selgelt, kontrollib RaMi ühisosakond andmekaitsetingimuste olemasolu, kuid see vajadus ei pruugi kavandist alati ilmneda. Varem koostatud andmetöötluslepingu vorm ei ole praegu keskselt kasutamiseks kättesaadav.

TRAMi töövõtulepingus olid paljud artikli 28 nõuded käsitletud, kuid alamtöötleja loa taotlemise ja dokumenteerimise protsess ei olnud detailselt kirjeldatud.

KeA ja KAURi tüüplepingutes ei olnud alati täpsemalt kirjeldatud töötlemise eesmärki ja ulatust, isikuandmete liike, andmesubjektide kategooriaid, töötlemise kestust, turvameetmeid, alamtöötlejate kaasamist ega andmete tagastamise või kustutamise korda.

ELMi valitud töövõtu- ja käsunduslepingutes ning RiLi vaadeldud raamlepingus sisaldusid üldised andmekaitse-, konfidentsiaalsus- või turvameetmete sätted, kuid töö käigus ei hinnatud täiendavalt, kas nende lepingute täitmisel toimus isikuandmete töötlemine asutuse nimel. Positiivne on, et RTK hankes valitsemisala asutustele korraldatud reisikorraldusteenuse leping sisaldab eraldi andmetöötluslepingut.

Kui lepingu ettevalmistamisel ilmneb, et teenuse osutamiseks töödeldakse isikuandmeid, tuleks hinnata poolte rolle ja teha kindlaks, kas lepingupartner töötleb andmeid asutuse nimel volitatud töötlejana või tegutseb muus rollis. Kui lepingupartner töötleb isikuandmeid asutuse nimel, tuleb lepingus või selle lisas sätestada GDPRi artikli 28 kohased tingimused. Kui isikuandmeid ei töödelda või lepingupartner ei tegutse volitatud töötlejana, ei ole artikli

28 tingimuste lisamine vajalik, kuid vastav kaalutlus peaks olema lepingu ettevalmistamisel teadlikult läbi mõeldud ja vajaduse korral dokumenteeritud.

JÄRELDUS 35 — volitatud töötlejate ülevaade, andmetöötlustingimused ja järelevalve. Kogutud teabe põhjal on volitatud töötlejate ülevaate ja järelevalve korraldus KliM valitsemisala asutustes erineva detailsusega.

TRAMis peetakse volitatud töötlejate arvestust teenusepõhiselt ning vastutus on teenusejuhtidel.

KAURis, RiLis ja KeMITis puudub terviklik koondülevaade volitatud töötlejate ning nende kaasatud teiste volitatud töötlejate kohta. KAURis ja RiLis kujuneb ülevaade volitatud töötlejatest isikuandmete töötlemise ülevaate koostamisel ja andmed kavandatakse kajastada isikuandmete töötlemise ülevaates.

KliMil ja KeAl on volitatud töötlejate kaasamise kohta osaline ülevaade ning kavandatud lahendusena nähakse teenusepõhiste nimekirjade pidamist ja andmete kajastamist töötlemisülevaates.

KeMITil on oma korras sätestatud andmekaitseaudit vähemalt kord nelja aasta jooksul, kuid mitmes asutuses ei ole volitatud töötlejate regulaarne vastavuse hindamine või järelevalve süsteemselt korraldatud ega dokumenteeritud. KliM ja KeA on kavandanud volitatud töötlejate kaasamise, andmetöötlustingimuste ning kontrolli täpsema reguleerimise. Kavandatud lahendused ei olnud töö läbiviimise ajal siiski veel täielikult kehtestatud ning asutustel puudub terviklik tegevuskava olemasolevate lepingute ülevaatamiseks ja vajaduse korral GDPRi artikli 28 nõuetega kooskõlla viimiseks.

Kui asutusel puudub ajakohane ülevaade nendest lepingupartneritest, kes tegelikult töötlevad isikuandmeid asutuse nimel, või kui selliste suhete puhul ei ole andmetöötlustingimused ja järelevalve piisavalt selgelt korraldatud, võib see raskendada vastutava töötleja kontrolli andmetöötluse üle ja GDPRi artikli 28 nõuete täitmise tõendamist. Seetõttu on oluline, et asutused seoksid volitatud töötlejate ülevaate, andmetöötlustingimuste olemasolu ja järelevalve korralduse töötlemisülevaate, lepinguregistri või muu sobiva töövahendiga ning hoiaksid seda teavet ajakohasena.

ETTEPANEKUD kõikidele asutustele:

39. Määrata hanke-, lepingu- või projektiprotsessis andmekaitsealane kontrollikoht, mille abil tehakse varases etapis kindlaks, kas kavandatava teenuse, lepingu, infosüsteemi, programmi, andmekogu või tööprotsessiga kaasneb isikuandmete töötlemine või volitatud töötleja kasutamine. Kontrollikoha raames määrata, millal kaasatakse AKS või muu andmekaitse eest vastutav roll, millist sisendit temalt oodatakse ning kuidas antud hinnang ja selle alusel tehtud otsused dokumenteeritakse. Kontrollikoht võib olla osa hankekorrast, lepingu kooskõlastamise korrast, arendusprotsessist või eraldi juhisest, kuid kehtestatud lahendus peaks olema praktikas rakendatav ning arvestama asutuse hangete mahtu, töökorraldust ja andmetöötluse riskitaset.
40. Töötada välja või võtta kasutusele GDPRi artikli 28 nõuetele vastav andmetöötluslepingu tüüplisa või tüüptingimused, mida kasutatakse juhul, kui lepingupartner töötleb isikuandmeid asutuse nimel. Tüüptingimused peavad hõlmama vähemalt töötlemise eset, kestust, laadi ja eesmärki, töödeldavate isikuandmete liike ja andmesubjektide kategooriaid, vastutava töötleja õigusi ja kohustusi, volitatud töötleja kohustust tegutseda dokumenteeritud juhiste alusel, konfidentsiaalsus- ja turvameetmeid, alamtöötlejate kaasamise tingimusi ja korda, isikuandmetega seotud rikkumistest teavitamist, andmesubjektide taotluste lahendamise ja auditite läbiviimise toetamist ning andmete ja nende koopiate tagastamist või kustutamist lepingu lõppemisel vastutava töötleja valikul ja selle kirjalikku tõendamist. Hinnata riskipõhiselt ka olemasolevaid lepinguid, et teha kindlaks, millistele lepingutele tuleb andmetöötlustingimused lisada või milliste lepingute tingimusi täiendada.
41. Koondada ja hoida ajakohasena ülevaade volitatud töötlejatest ning alamvolitatud töötlejatest, kajastades selles vähemalt töötleja seost konkreetse teenuse, infosüsteemi, andmestiku või tööprotsessiga, töödeldavate isikuandmete kategooriaid, töötlemise õiguslikku või lepingulist alust, andmetöötluslepingu või andmetöötlustingimuste olemasolu ning alamtöötlejate kasutamise lubamist ja dokumenteerimist. Ülevaade võib olla seotud isikuandmete töötlemise ülevaate, lepinguregistri või muu asutuses kasutatava töövahendiga, kuid määrata tuleb selle ajakohastamise eest vastutavad isikud või rollid ning ajakohastamise sagedus.
42. Kehtestada volitatud töötlejate riskipõhise järelevalve ja vastavuse hindamise põhimõtted, mille kohaselt hinnatakse enne volitatud töötleja kaasamist või lepingu sõlmimist tema võimet rakendada piisavaid tehnilisi ja korralduslikke meetmeid ning kontrollitakse lepingu kehtivuse ajal riskipõhiselt tema lepinguliste ja GDPRist tulenevate kohustuste täitmist. Kontrollide sageduse ja ulatuse määramisel arvestada töödeldavate isikuandmete laadi ja mahtu, andmetöötluse riskitaset, kasutatavat infosüsteemi, alamtöötlejate kasutamist ning varasemaid rikkumisi, puudusi ja muid juhtumeid. Dokumenteerida kontrollide tulemused, tuvastatud puudused, vajalikud parandusmeetmed, nende rakendamise tähtajad ja järelkontrolli tulemused.

Asutus	**Asutuse tagasiside** *(kajastatud on teemaploki kohta esitatud kommentaarid või asutuse üldine tagasiside aruande kohta)*

KliM	Nõustume ettepanekuga täpsustada andmekaitsenõuete arvestamist hanke-, lepingu- ja projektiprotsessides. Selleks on kavas välja töötada praktiline abivahend (dokument), mille abil saavad teised teenistujad hinnata, kas kavandatava tegevusega kaasneb isikuandmete töötlemine, kas on vaja sõlmida andmetöötlusleping, milliseid andmekaitseriske tuleb lepingupartneri puhul hinnata ning millal on vajalik AKSi kaasamine. Samuti on kavas välja töötada erinevatele andmetöötlussuhetele sobivad lepingumallid. Nõustume ka ettepanekuga vaadata riskipõhiselt üle olemasolevad lepingud ning hinnata nende vastavust andmekaitsenõuetele. Eelmainitud tegevustega peab kaasnema teenistujate teadlikkuse tõstmine. Hetkel puudub AKSi lepingute ülevaatamisse kaasamiseks kindel raamistik ning lepinguid on saadetud AKSile ülevaatamiseks pigem juhtumipõhiselt. Samuti on kavas luua ja ajakohasena hoida volitatud töötlejate ülevaade ning hinnata, milline lahendus on sellise ülevaate pidamiseks kõige sobivam ja praktilisem. Samuti peame oluliseks rõhutada ka aruandes mainitut, et AKSi kaasamine ei tähenda aga ärilise või juhtimisvastutuse ülevõtmist. Juhime samas tähelepanu sellele, et RaMi ühisosakond osutab KliMile hangete ja lepingutega seotud teenuseid. Praegu ei ole aga piisavalt selgelt piiritletud, millised lepingute kontrollid ja kohustused kuuluvad RaMi ühisosakonnale, millised KliMile, millised AKSile ning millises menetlusetapis vastavad kontrollid tehakse. Seetõttu oleks vajalik koostöös RaMi ühisosakonnaga täpsustada rollid ja vastutus ning kujundada selge töökorraldus, mis määraks kindlaks täpsema ülesannete ja vastutuse jaotuse.
TRAM	**Kommentaar ettepanekutele 39–42** Siinkohal leiame, et oleme ettepaneku eesmärgi täitnud, sest asutuse õigusosakond on välja töötanud isikuandmete töötlemise lepingute tüüptingimuste põhjad, mida täiendatakse vastavalt konkreetse andmetöötluslepingu eesmärgile ja sellest tulenevatele erisustele. Tüüptingimusi ajakohastatakse ja täiendatakse vastavalt muutuvatele vajadustele ning õigusaktidest tulenevatele nõuetele. Asutuses peetakse volitatud töötlejate arvestust teenusepõhiselt ning vastutavad teenusejuhid, kelle ülesannete hulka kuulub ka volitatud töötlejate üle järelevalve teostamine. Selline korraldus võimaldab hinnata volitatud töötlejatega seotud asjaolusid konkreetse teenuse kontekstis ning jälgida lepinguliste kohustuste täitmist.
KeA	KeA teavitas, et tal ei ole aruande kohta faktivigadele osutavaid märkusi. Aruandes esitatud ettepanekute kohta KeA täiendavaid kommentaare ei esitanud.
KAUR	Ettepanekuid arvestatakse asutuse protsesside ülevaatamisel. Tähtaeg ja vastutaja nimetatud ülal.
RiL	**Tagasiside aruande kohta tervikuna:** Üldises plaanis oleme järelduste ja ettepanekutega nõus. Mitmed tegevused, mida raportis välja toodud, olid auditi tegemise ajal juba töös ning nendega jätkame. Mõned täpsustused siiski. Esiteks võiks Riigilaevastiku tähelepanekute juures rohkem rõhutada proportsionaalsuse põhimõtet. Me ei halda riiklikke andmekogusid ega tegele suuremahulise isikuandmete töötlemisega ning seetõttu näeme enamiku tähelepanekute puhul pigem organisatsiooni küpsuse kasvatamise vajadust kui sisulist mittevastavust. Teiseks, AKSi töömahu hinnangut mõjutas olulisel määral töötlemistoimingute ülevaate koostamine ja auditi läbiviimine ise. Seetõttu ei pruugi auditi periood peegeldada tavapärast olukorda. Kolmandaks, koolituste osas vastab tõele, et süsteemset majasisest koolitusprogrammi ei ole veel olnud, kuid teadlikkust on tõstetud jooksva nõustamise kaudu ning töötajad on osalenud ka erinevatel väliskoolitustel ja seminaridel. Novembris ja detsembris viime läbi ka organisatsioonisisese koolituse kõikidele asutuse töötajatele. Lisaks märgiksin, et haldusala ühise siseveebi ja materjalide puudulik kättesaadavus ei ole olnud ainult RiLi tegevusetus, vaid tuleneb ka valitsemisala IT-tehnilisest korraldusest. Muus osas kommentaare ei ole ning täname veel kord põhjaliku ja konstruktiivse töö eest.
KeMIT	Nõus ettepanekutega. Hetkel KeMIT enam aktiivselt enda kordade uuendamisega ei tegele ning täpsem töökorraldus tuleb üle vaadata Riigi Digikeskuse loomise käigus.
EGT	EGT nõustub, et andmetöötlusrollid tuleb määrata konkreetse töötlemise järgi ning artikli 28 kohaseid tingimusi kasutatakse volitatud töötleja suhte korral. Toetame ühiselt kasutatava andmetöötluslepingu tüüplisa või tüüptingimuste koostamist. Kontrolli korraldus peab arvestama asutuse hangete mahtu, töökorraldust ja töötlemise riske.
ELM	**Tagasiside aruande kohta tervikuna:** Oleme aruande eelnõu läbi vaadanud ning Loodusmuuseumi puudutavate kirjelduste ja järelduste osas suuri ebakõlasid ei tuvastanud.

	AKSi ülesannete täitmise osas on meie jaoks peamine väljakutse vajaliku ressursi ja kompetentsi tagamine. Muuseumi praegune töökorraldus ja tänane töökoormus ei võimalda meil neid ülesandeid olemasolevate töötajate vahel jagada, sest andmekaitse teemad vajavad järjepidevat tähelepanu ja eraldi fookust. Seetõttu otsime praegu haldusala seest sobivat inimest, kes saaks AKSi ülesandeid täita, ning loodame leida lahenduse koostöös mõne teise haldusala asutusega.