LISA nr 1
KINNITATUD
Peadirektori KK nr1-1/12, 13.02.2026

Siseministeeriumi infotehnoloogia- ja arenduskeskuse isikuandmete töötlemise ja kaitse kord

1. **Üldsätted**

1.1 Isikuandmete töötlemise ja kaitse kord (edaspidi *kord*) sätestab isikuandmete töötlemise põhimõtted Siseministeeriumi infotehnoloogia- ja arenduskeskuses (edaspidi *SMIT*), andmesubjekti õigused ja SMITi, selle töötajate ja väliste partnerite kohustused isikuandmete töötlemisel.

1.2 SMIT töötleb isikuandmeid lähtudes Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärusest (Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta), isikuandmete kaitse seaduse (edaspidi *seadus*) ja teiste isikuandmete töötlemist ja kaitset reguleerivate õigusaktide nõuetest lähtuvalt. Korra väljatöötamisel on juhindutud Andmekaitse Inspektsiooni poolt seaduse rakendamiseks antud isikuandmete töötlemise ja kaitse alastest soovituslikest juhistest.

1.3 Kord avaldatakse SMITi avalikus dokumendiregistris ja veebilehel. Lisaks avaldatakse veebilehel korral põhinev SMITi andmekaitsetingimused, kus selgitatakse isikuandmete töötlemise tingimusi.

2. **Mõisted**

2.1 **Isikuandmed** – igasugune teave tuvastatud või tuvastatava füüsilise isiku *(„andmesubjekti")* kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

2.2 **Eriliiki isikuandmed** – andmed füüsilise isiku:

2.2.1 poliitiliste vaadete (v.a erakonna liikmelisus) kohta;

2.2.2 usuliste ja filosoofiliste veendumuste kohta;

2.2.3 rassilise või etnilise päritolu kohta;

2.2.4 terviseseisundi kohta;

2.2.5 pärilikkuse informatsiooni (geeniandmed) kohta;

2.2.6 biomeetrika (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis) kohta;

2.2.7 seksuaalelu ja seksuaalse sättumuse kohta;

2.2.8 ametiühingu liikmelisuse kohta;

2.2.9 süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

2.3 **Eraelulised isikuandmed** – isikuandmed, millele juurdepääsu võimaldamine võib kahjustada oluliselt füüsilise isiku eraelu puutumatust.

2.4 **Andmesubjekt** – füüsiline isik, kelle isikuandmeid töödeldakse.

2.5 **Isikuandmeid sisaldav teabekandja** – mis tahes objekt, millele on jäädvustatud isikuandmed.

2.6 **Isikuandmete töötlemine** – iga isikuandmetega automatiseeritud või automatiseerimata toiming, sealhulgas isikuandmete kogumine, dokumenteerimine, salvestamine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, lugemine ja

avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine, piiramine, või nende toimingute kombinatsioon, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

2.7 **Isikuandmete kaitse** – isikuandmete töötlemisel organisatsiooniliste, füüsiliste, tehniliste ja elektrooniliste teabeturbe meetmete rakendamine.

2.8 **Isikuandmete kaitse korraldamine** – isikuandmete töötlemise ja kaitse nõuetele vastavuse tagamine.

2.9 **Isikuandmete kaitset korraldav isik** – töötaja, kelle tööülesandeks on isikuandmete kaitse korraldamine.

2.10 **Isikuandmete infosüsteem** – infosüsteem, sealhulgas tehnilised vahendid, mida kasutatakse isikuandmete elektrooniliseks töötlemiseks.

2.11 **Juurdepääsuvajadusega isik** – füüsiline või juriidiline isik, riigi- või kohaliku omavalitsuse asutus, kellel on isikuandmetele juurdepääsuvajadus.

2.12 **Kolmas isik** – iga füüsiline või juriidiline isik, kes ei ole andmesubjekt, vastutav töötleja, volitatud töötleja ega nimetatud isikute töötaja.

2.13 **Volitatud töötleja** – isik või organisatsioon, kes töötleb isikuandmeid vastutava töötleja nimel ja juhiste järgi.

2.14 **Väline partner** – SMIT-le teenuseid osutav isik, või isik kellele SMIT osutab teenust (lepingupartner või organisatsioon jt).

3. Isikuandmete töötlemise ja kaitse nõuete täitmise eest vastutavad isikud

3.1 SMITis vastutavad isikuandmete töötlemise ja kaitse nõuete täitmise eest järgmised isikud oma pädevuse ja ülesannete ulatuses:

3.1.1 SMITi peadirektor vastutab isikuandmete töötlemise ja kaitse nõuete üldise täitmise eest ning tagab asutuses vastava korralduse olemasolu;

3.1.2 isikuandmete kaitset korraldav isik vastutab isikuandmete kaitse korraldamise, nõuete rakendamise ja asjakohase nõustamise eest kooskõlas Euroopa Liidu ja Eesti Vabariigi õigusaktidega;

3.1.3 isikuandmeid töötleva struktuuriüksuse juht (edaspidi *struktuuriüksuse juht*) vastutab isikuandmete töötlemise ja kaitse nõuete täitmise eest oma juhitavas struktuuriüksuses ning tagab töötajate teadlikkuse vastavatest nõuetest;

3.1.4 isikuandmeid töötlev töötaja (edaspidi *töötaja*) vastutab isikuandmete töötlemisel, sh isikuandmeid sisaldava teabekandja kasutamisel, talle kehtestatud isikuandmete töötlemise ja kaitse nõuete täitmise eest ning kohustub teatama viivitamata võimalikest rikkumistest.

4. SMITi peadirektor

4.1 Määrab isikuandmete kaitset korraldava isiku ning tagab talle oma ülesannete täitmiseks vajaliku sõltumatuse, volitused ja vahetu juurdepääsu asutuse juhtkonnale.

4.2 Tagab isikuandmete kaitset korraldavale isikule vajalikud ressursid ja võimalused erialase pädevuse säilitamiseks ning pidevaks täiendõppeks, et tagada ekspertteadmiste ajakohasus.

4.3 Vastutab isikuandmete töötlemise ja kaitse nõuete üldise täitmise eest ning tagab asutuses vastava korralduse olemasolu.

4.4 Kinnitab isikuandmete töötlemist ja kaitset reguleerivad sisemised õigusaktid ning tagab nende ajakohasuse.

4.5 Tagab, et isikuandmete töötlemine SMITis toimub kooskõlas kehtivate õigusaktide, sealhulgas isikuandmete kaitse üldmääruse ja riigisiseste õigusaktidega.

4.6 Tagab, et asutuse riskihalduse poliitika hõlmab isikuandmete töötlemise ja kaitsega seotud riskide juhtimist.

4.7 Tagab asutuses piisavate organisatsiooniliste, tehniliste ja rahaliste ressursside olemasolu isikuandmete töötlemise ja kaitse nõuete täitmiseks.

4.8 Saab regulaarselt ülevaate isikuandmete töötlemise ja kaitse seisust, sh olulisematest riskidest, rikkumistest ja rakendatud meetmetest.

4.9 Otsustab vajaduse korral isikuandmete töötlemisega seotud oluliste riskide vastuvõtmise või täiendavate meetmete rakendamise.
4.10 Tagab koostöö Andmekaitse Inspektsiooniga ning muude järelevalveasutustega strateegilisel tasandil.
4.11 Tagab, et isikuandmete kaitse on integreeritud asutuse strateegilisse juhtimisse ja tegevusplaneerimisse.

5. **Isikuandmete kaitset korraldav isik**
5.1 SMITi peadirektor määrab isikuandmete kaitse korraldamiseks isikuandmete kaitset korraldava isiku, kes:
5.1.1 kontrollib regulaarselt, et SMIT töötleks ja kaitseks isikuandmeid vastavalt seadusele ja käesolevale korrale ning teistele õigusaktidele;
5.1.2 võtab SMITis tarvitusele sobilikud meetmed isikuandmete töötlemise ja kaitse nõuetega vastavusse viimiseks;
5.1.3 omab isikuandmete töötlemisülevaadet. SMITis on isikundmete töötlemisülevaade seotud teabe hoiukohtade registriga (THR);
5.1.4 toetab andmekaitsealase mõjuhinnangu koostamisega;
5.1.5 esitab SMITi peadirektorile kord aastas ülevaate enda tegevusest, isikuandmete kaitsmiseks kavandatud meetmete rakendamise seisust ning töötajate andmekaitsealaste teadmiste testimise tulemustest;
5.1.6 esitab SMITi peadirektorile ülevaate isikuandmete töötlemisel toimunud rikkumisest esimesel võimalusel, tagades informatsiooni edastamise hiljemalt 72 tunni jooksul alates rikkumise tuvastamisest;
5.1.7 nõustab töötajaid igapäevaselt isikuandmete töötlemise ja kaitse küsimustes;
5.1.8 viib töötajatele regulaarselt läbi koolitusi isikuandmete töötlemise ja andmekaitse teemadel;
5.1.9 teavitab isikuandmete kaitset korraldava isiku määramisest Andmekaitse Inspektsiooni, teatades oma nime ja kontaktandmed;
5.1.10 on oma tegevuses sõltumatu;
5.1.11 koostab isikuandmete kaitse üldmäärusele vastavad andmekaitsetingimused, vaatab need üle vähemalt kord aastas ning ajakohastab vastavalt vajadusele, tagades nende vastavuse kehtivatele õigusaktidele ja SMITi andmetöötlusprotsessidele;
5.1.12 konsulteerib isikuandmete töötlemise ja isikuandmete kaitseks rakendatavate organisatsiooniliste, füüsiliste, tehniliste ja elektrooniliste teabeturbe meetmete osas Andmekaitse Inspektsiooniga;
5.1.13 palub asjaajamisosakonnal teha vastavad muudatused äriregistris, et sakis "Andmekaitsespetsialist" kajastuks isikuandmete kaitset korraldava isiku nimi.

6. **Juht**
6.1 Koordineerib isikuandmete töötlemist ja kaitset struktuuriüksuses käesoleva korra nõuete kohaselt.
6.2 Määrab kindlaks koostöös isikuandmete kaitset korraldava isikuga struktuuriüksuse isikuandmete töötlemise eesmärgid ja töödeldavate isikuandmete koosseisu.
6.3 Otsustab juurdepääsu võimaldamise struktuuriüksuse isikuandmeid sisaldavatele teabekandjatele ja isikuandmete edastamise kooskõlas seaduse ja teiste õigusaktidega, konsulteerides isikuandmete kaitset korraldava isikuga.
6.4 Tagab, et struktuuriüksuses puudub isikuandmetele ligipääs juurdepääsuõiguseta isikutel.
6.5 Tagab, et struktuuriüksuse töötajad on teadlikud isikuandmete töötlemise ja kaitse nõuetest ning korraldab vajaduse korral töötajate juhendamise ja koolitamise koostöös isikuandmete kaitset korraldava isikuga.
6.6 Jälgib ja kontrollib struktuuriüksuses isikuandmete töötlemise vastavust kehtivatele nõuetele ning rakendab rikkumiste või puuduste ilmnemisel parandusmeetmeid.

6.7 Võib lubada töötajal töödelda eraelulisi isikuandmeid sisaldavaid teabekandjaid väljaspool SMITi ruume, kui see on kooskõlastatud eelnevalt isikuandmete kaitset korraldava isiku ja infoturbejuhiga.
6.8 Kooskõlastab isikuandmete kaitseks rakendatavad organisatsioonilised, füüsilised, tehnilised ja elektroonilised teabeturbe meetmed isikuandmete kaitset korraldava isikuga.
6.9 Osaleb isikuandmete töötlemise riskide hindamisel ja mõjuanalüüside läbiviimisel, kui struktuuriüksuse tegevus seda nõuab.
6.10 Tagab isikuandmete töötlemise lõpetamisel või töötaja teenistussuhte lõppemisel juurdepääsuõiguste õigeaegse muutmise või lõpetamise.
6.11 On kohustatud teavitama:
6.11.1 isikuandmeid sisaldavate teabekandjate edastamise, hoiustamise, säilitamise ja hävitamise kaitse meetmete ebapiisavuse korral siseaudiitorit ja isikuandmete kaitset korraldavat isikut;
6.11.2 isikuandmete infosüsteemi isikuandmete kaitse meetmete ebapiisavuse korral vastava isikuandmete infosüsteemi peakasutajat ja isikuandmete kaitset korraldavat isikut;
6.11.3 isikuandmete töötlemise ja kaitse nõuete rikkumise korral isikuandmete kaitset korraldava isikut.

7. **Töötaja**
7.1 Töötaja töötleb isikuandmeid sisaldavaid teabekandjaid korra nõuete kohaselt.
7.2 Rakendab isikuandmete töötlemisel isikuandmete kaitseks nõuetekohaseid organisatsioonilisi, füüsilisi, tehnilisi ja elektroonilisi teabeturbe meetmeid, et ära hoida isikuandmete volitamata töötlemist.
7.3 Tagab, et isikuandmete töötlemise ruumis on välditud:
7.3.1 juurdepääsuõiguseta isikute ligipääs isikuandmetele;
7.3.2 isikuandmeid sisaldavate teabekandjate omavoliline teisaldamine.
7.4 Tagab, et isikuandmed ei saaks edastamise käigus teatavaks juurdepääsuõiguseta isikule.
7.5 Töötajal tuleb isikuandmeid sisaldava teabekandja SMITi ruumidest väljaviimisel rakendada infoturbe meetmeid, et isikuandmed ei satuks juurdepääsuõiguseta isiku kätte.
7.6 Tagab, et isikuandmete edastamisel või transportimisel ei toimu isikuandmete volitamata lugemist, kopeerimist või hävitamist.
7.7 Tagab isikuandmeid sisaldava elektroonilise teabekandja puhul, et peale kasutuselt kõrvaldamist on elektrooniliselt teabekandjalt andmed turvaliselt kustutatud. Kasutuselt kõrvaldatud elektroonilised teabekandjad, millelt ei ole võimalik andmeid elektrooniliselt kustutada, tuleb hävitada füüsiliselt.
7.8 Kohustub osalema isikuandmete andmekaitse jätkukoolitusel üks kord aastas. Uus töötaja kohustub esimesel andmekaitse sisekoolitustel osalema esimese 4 kuu jooksul alates tööle asumisest.
7.9 Kohustub isikuandmete töötlemise ja kaitse nõuete alase küsimusega pöörduma isikuandmete kaitset korraldava isiku poole.
7.10 kohustatud talle teatavaks saanud isikuandmete töötlemise ja kaitse nõuete rikkumisest koheselt teavitama struktuuriüksuse juhti ja isikuandmete kaitset korraldavat isikut.
7.11 kohustatud hoidma saladuses talle tööülesannete täitmisel teatavaks saanud isikuandmeid ka pärast isikuandmete töötlemisega seotud tööülesannete täitmist või töösuhte lõppemist vastavalt õigusaktides sätestatud tähtaegadele.

8. **Väline partner**
8.1 Saab juurdepääsu isikuandmeid sisaldavale teabele ainult lepingu täitmisega seotud ülesannete täitmiseks.
8.2 Tagab, et on teadlik ja tagab, et täidab kõiki kehtivaid isikuandmete töötlemisalaseid nõudeid, andmete turvalisust puudutavaid ning isikuandmete kaitse alaseid Euroopa Liidu ja Eesti Vabariigi õigusakte ja muid eeskirju.
8.3 Kohustub rakendama järgmisi organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid teabe kaitseks juhusliku või tahtliku volitamata muutmise, juhusliku hävimise ja tahtliku

hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest, volitamata töötlemise, sh avalikustamise eest:

8.3.1 vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele;

8.3.2 ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis, samuti andmekandjate omavolilist teisaldamist;

8.3.3 ära hoidma isikuandmete omavolilist salvestamist, muutmist ja kustutamist ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi;

8.3.4 tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks;

8.3.5 tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja milliseid isikuandmeid edastati ning samuti selliste andmete muutusteta säilimise;

8.3.6 tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist ja/või kustutamist.

8.4 Kohustub teavitama toimunud või põhjendatult kahtlustatavast isikuandmete töötlemise rikkumisest, mis põhjustab, on põhjustanud või võib põhjustada edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu, kirjalikult viivitamata, kuid mitte hiljem kui 24 tundi pärast sellest teada saamist aadressil andmekaitse@smit.ee

8.5 Tulenevalt lepingu esemest on SMITil õigus seada täiendavaid nõudeid ja/või juhiseid isikuandmete töötlemiseks.

9. **Isikuandmete töötlemise põhimõtted**

9.1 **Seaduslikkuse põhimõte** – isikuandmeid võib koguda vaid ausal ja seaduslikul teel ning igasuguseks isikuandmete töötlemiseks peab olema alus.

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

9.3 **Minimaalsuse põhimõte** – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.

9.4 **Kasutuse (säilitamise) piiramise põhimõ**te – isikuandmeid võib kasutada üksnes eesmärgipäraselt ja eesmärgi saavutamiseni, eesmärgist tuleneb ka säilitamistähtaeg. Isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal.

9.5 **Õigsuse ja andmete kvaliteedi põhimõte** – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks.

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

9.7 **Vastutuse ja läbipaistvuse põhimõte** – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

9.8 Lähtudes korras toodud isikuandmete töötlemise põhimõtetest, SMIT:

9.8.1 töötleb isikuandmeid, sh edastab neid kolmandale isikule ja/või kolmandasse riiki, ainult seaduse, lepingu, nõusoleku või õigustatud huviga määratud eesmärgil ja ulatuses järgides kõiki andmekaitset reguleerivaid õigusakte;

9.8.2 tagab isikuandmete kaitse läbi tõhusate organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete (nt edastab selliseid andmeid krüpteeritult) ning range konfidentsiaalsus- ja turvalisusreeglistiku, kaitstes isikuandmeid igasuguse õigustamatu kasutamise eest;

9.8.3 tunnistab isikuandmeid sisaldava teabe asutusesiseseks kasutamiseks mõeldud teabeks ja kehtestab sellele juurdepääsupiirangu;

9.8.4 kustutab või hävitab viivitamata isikuandmeid, mida SMIT enam ei vaja, sh säilitustähtaja möödumise tõttu (kui ei esine kohustust nende säilitamiseks);

9.8.5 võimaldab ligipääsu isikuandmetele ainult vastava juhendamise saanud töötajatele ja muudele volitatud isikutele, kellel on õigus isikuandmeid töödelda vaid ulatuses, mis on vajalikud isikuandmete töötlemise eesmärkide saavutamiseks;

9.8.6 ei väljasta isikuandmeid kolmandatele isikutele, välja arvatud juhul kui andmete väljastamise kohustus tuleneb seadusest või andmesubjekt on andnud selleks loa.

10. Turvameetmed isikuandmete kaitseks

10.1 Isikuandmete kaitseks rakendatavate turvameetmete eesmärk on kaitsta:

10.1.1 juhusliku või tahtliku volitamata muutmise eest;

10.1.2 juhusliku ja/või tahtliku hävitamise eest;

10.1.3 volitamata töötlemise (sh volitamata juurdepääsu) eest.

10.2 SMITi poolt töödeldavad isikuandmed on peamiselt paberkandjal dokumentidena, digitaalkujul andmekandjatel või infosüsteemides sh SMITi dokumendihaldussüsteemis, riigi personali- ja palgaarvestuse andmekogus, millele ligipääsemiseks kasutatakse unikaalseid kasutajatunnuseid ja paroole ning on tagatud, et vastava infosüsteemi kasutajal on ligipääs üksnes tema tööülesannete täitmiseks vajalikele andmetele.

10.3 Eriliigilisi isikuandmeid sisaldavaid paberdokumente või teisaldatavaid andmekandjaid hoitakse ja säilitatakse SMITi lukustatavates kappides ning muudes turvalistes hoiukohtades.

10.4 Eriliigilisi isikuandmeid sisaldavad paberdokumendid või teisaldatavad andmekandjad utiliseeritakse, kui SMIT neid enam ei vaja, sh dokumentide säilitustähtaja möödumisel.

11. Isikud, kelle andmeid SMIT töötleb

11.1 Andmesubjektid, kes kasutavad SMITi hallatavaid teenuseid ja infosüsteeme: isikud, kelle andmete töötlemine on vajalik SMITi põhimäärusest tulenevate ülesannete täitmiseks (sh siseturvalisuse valdkonna IKT-teenuste osutamine, infosüsteemide arendamine, haldamine ning kasutajatoe pakkumine).

11.2 Koostööpartnerite ja hankijate kontaktisikud ning esindajad: füüsilised isikud, kes esindavad SMITi lepingulisi partnereid või on määratud nende poolseteks kontaktisikuteks teenuste osutamise või kaupade tarnimise raames.

11.3 Volitatud kontaktisikud: kolmandad isikud, keda andmesubjekt on ise määranud enda nimel suhtlema või kelle andmed on edastatud sidekanali kaudu teate edastamiseks.

11.4 SMITi poole pöörduvad isikud: isikud, kes esitavad SMITile selgitustaotlusi, märgukirju või teabenõudeid ning kelle andmeid töödeldakse vastuse koostamiseks.

11.5 Külastajad ja viibijad SMITi objektidel: isikud, kelle andmeid (nt nimi, isikukood, kujutis) töödeldakse SMITi hallatavatele objektidele pääsu reguleerimiseks või turvalisuse tagamiseks (sh videovalve).

11.6 Töötajad ja tööle kandideerijad: isikud, kes töötavad või on töötanud SMITis (sh teenistujad ja praktikandid) või kes on esitanud kandideerimisavalduse vabale ametikohale ning kelle andmeid töödeldakse töö- või teenistussuhte täitmiseks, personaliarvestuse pidamiseks või värbamisprotsessi läbiviimiseks.

12. Isikuandmete töötlemise eesmärk

12.1 Põhitegevusega seotud teenuste osutamine: siseturvalisuse valdkonna infosüsteemide arendamine, haldamine ja kasutajatoe pakkumine, et tagada operatiivteenistustele vajalik IKT-tugi.

12.2 Lepingute sõlmimine ja täitmine: koostööpartnerite ja hankijate kontaktisikute ning esindajatega suhtlemine ning lepinguliste kohustuste täitmine.

12.3 Turvalisuse tagamine: SMITi objektide, vara ja infosüsteemide kaitse (sh läbipääsusüsteemid ja videovalve).

12.4 Päringutele vastamine: isikute selgitustaotlustele, märgukirjadele ja teabenõuetele vastamine seadusega sätestatud korras.

12.5 Personalitöö ja värbamine: töö- ja teenistussuhete haldamine ning sobivate kandidaatide leidmine vabadele ametikohtadele.

12.6 Seadusest tulenevate kohustuste täitmine: muude SMITi põhimäärusest või õigusaktidest tulenevate avalike ülesannete täitmine.

13. **Peamine töödeldavate isikuandmete koosseis**

13.1 Isikutuvastusandmed: nimi, isikukood, sünniaeg, foto (töötõendil ja/või infosüsteemides), kodakondsus, rahvus.

13.2 Kontaktandmed: e-posti aadress, mobiiltelefoni või telefoninumber, postiaadress;

13.3 Tööalase tegevuse ja kvalifikatsiooni andmed: hariduskäik, töökogemus, läbitud koolitused, sertifikaadid, ametikohtade ajalugu, hoiatused ehk töökohustuste rikkumist kirjeldav info, arenguvestluste kokkuvõtted ja töösoorituse hinnangud, teave eelistatud teiste kasutatavate võõrkeelte ja nende taseme kohta.

13.4 Finantsandmed: arvelduskonto number, andmed töötasu, kogumispensioni, puhkusetasude, hüvitiste, päevarahade ja kinnipeetud maksude ja maksuarvestuse kohta.

13.5 Julgeoleku- ja usaldusväärsuse andmed: teave julgeolekukontrolli läbimise ja riigisaladuse loa olemasolu ja tulemuse kohta, andmed karistatuse kohta (seaduses sätestatud juhtudel ja mahus).

13.6 Perekondlikud ja sotsiaalsed andmed: teave perekonna ja ülalpeetavate kohta (nt laste andmed täiendava puhkuse/jõulukingi saamiseks), perekonnaseis (nt kui kontaktisikuks on määratud abikaasa), kontaktisik eriolukorras.

13.7 Teave teise tööandja juures töötamise kohta: kõrvaltegevuse teavitused ning riigisaladuse loa ja/või välisteabele juurdepääsu sertifikaatide haldamisega seotud andmete edastamine töösuhte lõppemisel.

13.8 Eriliigilised isikuandmed (terviseandmed): teave terviseseisundi kohta, töövõime kaotuse protsent ja puude raskusaste (arstliku ekspertiisi otsuse alusel seadusest tulenevate soodustuste või töötingimuste kohandamiseks), teave töövõimetuslehtede ja tööõnnetuste kohta, teave töötaja lapse kohta (nt puudega lapse lapsevanema puhkusepäevad)

13.9 Digitaalsed ja tehnilised andmed: kasutajanimed, süsteemipääsude õigused, infosüsteemide kasutuslogid, uksekaardi kasutamise andmed ning tööalane e-kirjavahetus.

13.10 Visuaalsed andmed: videovalve salvestised SMITi hallatavatel objektidel turvalisuse tagamiseks.

13.11 Isikliku sõiduki andmed (kui need on parkimiskoha/kulude hüvitamise taotlemiseks esitatud).

14. **Isikuandmete edastamine või nendele juurdepääsu võimaldamine andmete töötlemiseks kolmandale isikule on lubatud andmesubjekti nõusolekuta juhul, kui:**

14.1 Isikuandmed laekuvad ja neid töödeldakse isikustamata kujul (nt anonüümsed küsitlused).

14.2 Üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada.

14.3 Isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks.

14.4 SMIT avalikustab avaliku teabe seaduse alusel teabe ja/või dokumendid oma kodulehel või edastab isikule teabe ja/või dokumendi teabenõude alusel. Juurdepääsu piiramisel lähtub avaliku teabe seaduse §-st 35. Andmesubjektiga seotud dokumendid on valdavalt juurdepääsupiiranguga, avalikus dokumendiregistris kasutatakse andmesubjekti nime asemel initsiaale, dokumendi pealkiri näidatakse kujul, mis ei võimalda aimata selle täpsemat sisu ja seal ei kuvata juurdepääsupiiranguga dokumendi sisu. Juurdepääsupiirangutega on võimalik tutvuda dokumentide loetelus. Kui isik on oma pöördumise või SMITi tegevusega seotud asjaolud ise isikuliselt avalikustanud, on SMITil õigus anda avalikkusele selgitusi, et tagada teabe tõesus ja asutuse tegevuse läbipaistvus.

15. **Läbipääsusüsteemid ja jälgimisseadmestik**

15.1 SMITi hoonetes kasutatavates läbipääsusüsteemides ja jälgimisseadmestikus töödeldakse isikuandmeid isikute läbipääsu ja vara turvalisuse tagamise eesmärgil. Muudel eesmärkidel võib läbipääsusüsteemi ja jälgimisseadmestiku isikuandmeid töödelda ainult infoturbejuhi ja isikuandmete kaitset korraldava isiku kirjalikul loal.

15.2 SMITi hoonetes ja territooriumidel vara kaitseks isikuandmeid edastavast ja salvestavast jälgimisseadmestikust informeeritakse isikuid vastavatel teavitussiltidel.

16. **SMIT võib isikuandmeid töödelda andmesubjekti nõusolekuta:**

16.1 Avaliku ülesande täitmiseks: töötlemine on vajalik SMITi põhimäärusest või muudest õigusaktidest tulenevate avalikes huvides olevate ülesannete täitmiseks (nt sisejulgeoleku valdkonna IKT-teenuste osutamine ja infosüsteemide haldamine).

16.2 Juriidilise kohustuse täitmine: töötlemine on vajalik seadusest tuleneva kohustuse täitmiseks (nt vastamine teabenõuetele või audititele).

16.3 Lepingu täitmine: töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt isiku taotlusele (v.a eriliigiliste isikuandmete töötlemine, milleks on vajalik eraldi õiguslik alus).

16.4 Õigustatud huvi korral: töötlemine on vajalik SMITi või kolmanda isiku õigustatud huvi korral (nt turvalisuse tagamine, videovalve kasutamine vara kaitseks, küberintsidentide lahendamine), tingimusel et andmesubjekti huvid või põhiõigused ei kaalu üles SMITi huve.

16.5 Eluliste huvide kaitseks: töötlemine on vajalik andmesubjekti või mõne teise füüsilise isiku eluliste huvide (elu, tervis, vabadus) kaitseks olukorras, kus andmesubjektilt ei ole võimalik nõusolekut saada.

17. **Isikuandmete töötlemisega seoses andmesubjekt:**

17.1 Võib isikuandmete töötluseks antud nõusoleku igal ajal tagasi võtta, esitades vastavasisulise avalduse andmekaitse@smit.ee, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud isikuandmete töötlemise seaduslikkust.

17.2 Võib saada SMIT-lt kinnitust selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse.

17.3 kui töödeldakse, siis saada teavet töödeldud isikuandmete, nende töötlemise eesmärkide ja liikide kohta. Kui teavet edastati kolmandatele isikutele ja/või kolmandatesse riikidesse, siis informatsiooni ka selle kohta.

17.4 Võib nõuda tema ebaõigete isikuandmete parandamist, mittetäielike andmete täiendamist, isikuandmete töötlemise piiramist vastavalt õigusaktidele.

17.5 Võib nõuda teda käsitlevate isikuandmete kustutamist, väljaarvatud juhul, kui SMIT-l või kolmandal isikul on õiguslik alus nende isikuandmete töötlemiseks.

17.6 Võib nõuda isikuandmete ülekandmist vaid siis, kui see on tehniliselt teostatav, st kui kaks süsteemi suudavad omavahel turvaliselt suhelda ja vastuvõttev süsteem on tehniliselt suuteline sissetulevaid andmeid vastu võtma.

17.7 Võib esitada vastuväiteid isikuandmete töötlemise suhtes kui see toimub SMITi või kolmanda isiku õigustatud huvi alusel. Välja arvatud juhul, kui on tõendatud, et andmeid töödeldakse mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti huvid, õigused ja vabadused, või kui andmeid töödeldakse õigusnõuete koostamise, esitamise või kaitsmise eesmärgil.

17.8 Võib saada teavet tema isikuandmetega seotud rikkumistest, kui rikkumine kujutab endast tõenäoliselt suurt ohtu tema õigustele ja vabadustele. SMIT peab vastavas teates selges ja lihtsas keeles kirjeldama rikkumise laadi ning esitama andmekaitsespetsialisti või muu pädeva isiku nime ja kontaktandmed või kirjeldama rikkumise võimalikke tagajärgi või informeerima võimaliku kahjuliku mõju leevendamiseks rakendatud/kavandatud meetmetest.

17.9 Võib isikuandmete töötlemisega seonduvate küsimuste tekkimisel või kaebuse esitamiseks pöörduda SMITi poole kirjalikul teel alljärgnevatel kontaktidel: Mäealuse 2/2, Tallinn 12618, Eesti või e-posti aadressil andmekaitse@smit.ee.

18. **Avaldus oma andmetega tutvumiseks**

18.1 SMIT edastab isikuandmeid andmesubjektile või kolmanda isikule avalduse, lepingu, seaduse või seaduse alusel antud õigusakti alusel. Isikuandmeid sooviv isik peab suutma tõendada oma isikusamasust (digitaalselt allkirjastatud avaldus) ja andmete saamise õigust. Avaldus ja leping isikuandmete edastamiseks peavad olema kirjalikus vormis. Kui SMIT ei ole veendunud, et andmete edastamine on õigustatud, andmeid ei väljastata. Avaldus rahuldatakse või sellele esitatakse põhjendatud keeldumine seadusega ettenähtud tähtaja jooksul. Kui avaldust on vaja täpsustada või kui isikuandmete töötlus on aeganõudev, võib SMIT avalduse täitmise tähtaega pikendada informeerides sellest avalduse esitajat. SMIT võib keelduda teabe edastamisest, kui see võib:

18.1.1 takistada või kahjustada süüteo tõkestamist, avastamist või menetlemist või karistuse täideviimist;

18.1.2 kahjustada teise isiku õigusi ja vabadusi;

18.1.3 ohustada riigi julgeolekut;

18.1.4 ohustada avaliku korra kaitset;

18.1.5 takistada ametlikku uurimist või menetlust.

19. **Andmekaitsekoolituse põhimõtted**

19.1 SMIT tagab töötajatele isikuandmete kaitse alase juhendamise ja koolituse nii tööleasumisel kui ka regulaarselt kogu teenistussuhte jooksul. Koolituste eesmärk on tagada töötajate teadlikkus kehtivatest nõuetest ja ennetada andmekaitsealaseid vahejuhtumeid.

19.2 Iga uus töötaja on kohustatud läbima andmekaitsealase sissejuhatava koolituse esimese 2 kuu jooksul pärast tööle asumist. Koolituse läbimine on eelduseks iseseisvale andmetöötlusele ja juurdepääsuõiguste säilitamisele.

19.3 Andmekaitsealase sissejuhatava koolituse edukas läbimine ettenähtud tähtaja jooksul on üks osa töötaja katseaja eesmärkide täitmisest. Juhul kui töötaja ei ole koolitust läbinud hiljemalt katseaja lõpuks endast tulenevatel põhjustel (nt korduv eiramine, testimisest hoidumine), võidakse katseaeg lugeda juhi otsusel mitteläbituks.

19.4 Töötajate teadmiste värskendamiseks ja ajakohastamiseks toimub andmekaitsealane jätkukoolitus kord aastas Coursy keskkonnas. Koolituse sisu ja fookusteemad võivad aastati varieeruda vastavalt aktuaalsetele riskidele või muudatustele töökorralduses.

19.5 Jätkukoolituse läbimist kontrollitakse teadmiste testiga. Test loetakse edukalt sooritatuks, kui töötaja on vastanud õigesti vähemalt 80% küsimustest. Testi sooritamise ja tulemused fikseerib SMIT viisil, mis võimaldab tagantjärele kontrollida töötaja pädevuse vastavust kehtestatud nõuetele.

19.6 Juhul kui töötaja ei soorita jätkukoolituse testi kolmel järjestikusel korral:

19.6.1 peatab vahetu juht ajutiselt töötaja isikuandmete töötlemise õiguse ja juurdepääsu vastavatele infosüsteemidele;

19.6.2 töötajale määratakse kohustuslik personaalne täiendjuhendamine otsese juhi või isikuandmete kaitset korraldava isiku poolt;

19.6.3 pärast täiendjuhendamist sooritatud testi korduvat ebaõnnestumist võidakse käsitleda seda töökohustuste rikkumisena või ametikohale sobimatusena, mis võib tuua kaasa töösuhte lõpetamise.

20. **Töötajate andmekaitsealane pädevus**

20.1 Töötajad on kohustatud tundma ja järgima isikuandmete kaitset reguleerivaid õigusakte ning asutuse sisemisi andmekaitse- ja infoturbealaseid õigusakte.

20.2 SMITi kõikidel töötajatel peab olema ametikohale vastav piisav teadlikkus isikuandmete kaitse reeglitest ja küberturvalisuse põhitõdedest, töötajad peavad omama isikuandmete

töötlemiseks vajalikku pädevust vastavalt oma ametikoha ülesannetele. Soovitud üldpädevus hõlmab:

20.2.1 isikuandmete liikide (tava- ja eriliigilised andmed) eristamist;
20.2.2 andmetöötluse üldpõhimõtete (sh eesmärgipärasus ja minimaalsus) tundmist;
20.2.3 oskust tuvastada isikuandmetega seotud rikkumist või selle ohtu;
20.2.4 teadmist, kuidas ja kellele rikkumisest viivitamatult teavitada.

21. Andmekaitsealase pädevuse kontrollimine

21.1 SMIT korraldab töötajate isikuandmete kaitse alase pädevuse kontrollimist.
21.2 Andmekaitse jätkukoolitus lõppeb testiga, kuid pädevust võib lisaks kontrollida testide, teadmiste hindamise, juhendite järgimise kontrolli või muude asjakohaste meetodite kaudu.
21.3 Pädevuse kontrollimise ja koolituste läbiviimisega seotud teave dokumenteeritakse.

22. SMIT meedias ja sotsiaalmeedias

22.1 Avalikkuse teadlikkuse suurendamiseks kajastab SMIT uudiseid ja fotosid oma ülesannete täitmisest oma veebilehel, siseveebis ning muudes meediakanalites. Isikuandmete töötlemisel lähtutakse eesmärgipärasuse ja minimaalsuse põhimõttest ning hoidutakse asjaosaliste eraelu ülemäärasest riivamisest.
22.2 Füüsiliste isikute jäädvustamine (heli-, foto- või videosalvestised) ja nende avaldamine SMIT-i kanalites toimub:
22.2.1 andmesubjekti nõusoleku alusel, mis on antud kirjalikku taasesitamist võimaldavas vormis;
22.2.2 avaliku ürituse raames, kus on tagatud inimeste eelnev teavitamine salvestamisest (nt sildid ürituse sissepääsu juures või kutsel olev teavitus). Avalikul üritusel pildistamisel on õiguslikuks aluseks SMIT-i õigustatud huvi teavitada avalikkust oma tegevusest.
22.3 Alaealiste isikute kujutiste jäädvustamisel ja avaldamisel on nõutav lapse seadusliku esindaja (lapsevanem/eestkostja) eelnev kirjalik nõusolek. Erandina on lubatud alaealiste jäädvustamine avalikel üritustel üldvaadetena, vältides lapse fokuseeritud ja selgelt tuvastatavat kujutamist.
22.4 Igaühel on õigus esitada vastuväide enda kujutise avaldamise kohta või võtta antud nõusolek tagasi. Vastava teavituse saamisel on kommunikatsiooniosakond kohustatud viivitamatult, kuid mitte hiljem kui 5 tööpäeva jooksul, antud salvestised SMIT-i hallatavatest kanalitest eemaldama või isiku kujutise hägustama (anonümiseerima).
22.5 Kolmandate osapoolte platvormidel (nt Facebook, Instagram, LinkedIn) andmete avaldamisel selgitab SMIT andmesubjektile, et andmete eemaldamine SMIT-i lehelt ei pruugi tähendada andmete täielikku kustumist platvormi serveritest või kolmandate isikute jagatud postitustest.

23. Rikkumiste lahendamine

23.1 Isikuandmetega seotud rikkumine on mistahes turvanõuetega seotud rikkumine, mis põhjustab isikuandmete:
23.1.1 lubamatu hävimise, kaotsimineku või muutmise;
23.1.2 lubamatu avalikustamise või lubamatu juurdepääsu võimaldamise selleks volitamata isikutele olenemata sellest, kas rikkumine toimus tahtlikult või juhuslikult.
23.2 Isikuandmete töötlemise ja kaitse nõuete rikkumise avastamisel võtab isikuandmete kaitset korraldav isik koheselt kasutusele vajalikud meetmed rikkumisest põhjustatava kahju piiramiseks ja edasise rikkumise vältimiseks.
23.3 Isikuandmete kaitset korraldaval isikul on õigus isikuandmete töötlemise ja kaitse nõuete rikkumise avastamisel anda struktuuriüksuse juhile korraldus isikuandmete töötlemise ajutiseks peatamiseks vastavas struktuuriüksuses.
23.4 sikuandmete kaitset korraldav isik võtab seletuse isikult, kes on rikkunud isikuandmete töötlemise ja kaitse nõudeid, ning dokumenteerib rikkumise asjaolud.

23.5 Isikuandmete kaitset korraldav isik edastab isikuandmete töötlemise ja kaitse nõudeid rikkunud töötajale ning struktuuriüksuse juhile ettepanekud isikuandmete töötlemise ja kaitse nõuete rikkumise kõrvaldamiseks ning edaspidiste rikkumiste ennetamiseks.

23.6 Isikuandmete kaitset korraldav isik teavitab isikuandmete töötlemise ja kaitse nõuete rikkumisest ja selle kõrvaldamiseks tehtud ettepanekutest SMITi peadirektorit.

23.7 SMITi peadirektor annab korraldusi isikuandmete töötlemise ja kaitse nõudeid rikkunud struktuuriüksuse juhile rikkumise kõrvaldamiseks ning vajalike meetmete rakendamiseks.

23.8 Isikuandmete töötlemise ja kaitse parendamiseks esitab isikuandmete kaitset korraldav isik struktuuriüksuse juhile ettepanekud sobilike organisatsiooniliste, tehniliste ja füüsiliste turvameetmete rakendamiseks.

23.9 Isikuandmete kaitset korraldav isik teostab järelkontrolli isikuandmete töötlemise ja kaitse nõuete rikkumise kõrvaldamise üle struktuuriüksuses ning dokumenteerib kontrolli tulemused.

23.10 Juhul, kui isikuandmete töötlemise ja kaitse nõuete rikkumise kõrvaldamiseks ei ole struktuuriüksuses võetud tarvitusele vajalikke meetmeid, teavitab isikuandmete kaitset korraldav isik rikkumisest SMITi peadirektorit ja Andmekaitse Inspektsiooni.

23.11 Isikuandmete töötlemise ja kaitse nõuete eiramisel võidakse isik võtta vastutusele vastavalt kehtivatele õigusaktidele.

23.11.1 Kui rikkumine põhjustas või tõenäoliselt põhjustab ohtu andmesubjektide õigustele ja vabadustele, kohustub isikuandmete kaitset korraldav isik esitama rikkumisteate Andmekaitse Inspektsioonile hiljemalt 72 tunni jooksul pärast rikkumise avastamist;

23.11.2 Kui rikkumine põhjustas või tõenäoliselt põhjustab andmesubjektidele suure kahju (sh oht inimese elule, tervisele, varale või mainele), kohustub isikuandmete kaitset korraldav isik rikkumisest teavitama ka andmesubjekti;

23.11.3 Juhul, kui SMIT on rikkumise tuvastamisel isikuandmete volitatud töötleja, kohustub asjakohane osakonna- või tiimijuht koostöös isikuandmete kaitset korraldava isikuga viivitamata teavitama vastutavat töötlejat (sh peakasutajat ja andmekaitsespetsialisti).