Isikuandmete töötlemise õiguspärasuse tagamise süsteemi loomine Justiitsministeeriumi näitel.

Justiitsministeeriumis on süsteemi või standardina, kuidas JM-is ja JM-i haldusalas isikuandmete töötlemise õiguspärasust tagada aluseks võetud ISKE väljatöötamisel ja arendamisel aluseks olnud Saksamaa BSI (saksa k. *Bundesamt für Sicherheit in der Informationstechnik*, inglise k. *Federal Office for Information Security*) poolt avaldatava infoturbe standardi - IT Baseline Protection Manual (saksa k. IT-Grundschutz) isikuandmete kaitse moodulis B1.5 ettenähtud meetmete rakendamine. Üldjoontes järgib isikuandmete kaitse moodul etalonturbe süsteemi loogikat ning näeb ette konkreetsed meetmed isikuandmete töötlemise õiguspärasuse tagamiseks ning määratleb ka iga meetme eest vastutajad ja algatajad.

Uuem IT Baseline Protection Manual`i 2014.a versioon (IT-Grundschutz-catalogues 14th version – 2014. Lisa 8. GSK_14_EL_EN_Draft), on leitav aadressil: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_14_EL_EN_Draft.pdf?__blob=publicationFile&v=4 ning isikuandmete kaitse moodulit on käsitletud lehekülgedel 68 – 72 ja meetmeid lehekülgedel 2453 – 2484.

Samas jälle ISKE meetmete kataloogi versiooni 8.02. mingis versioonis on kõik andmekaitse mooduli B 1.5. meetmed olema ning ka tõlgitud. Seega tuleks lähtuda ikkagi ISKE tõlkest ning minu BSI tõlget mitte kasutada.

ISKE meetmete kataloogi versiooni 8.03 andmekaitse mooduli B 1.5. meetmed:

- M 2.501 **Isikuandme**te kaitse haldus
- M 2.502 **Isikuandme**te kaitse vastutusalade kindlaksmääramine
- M 2.503 **Isikuandme**te kaitse kontseptsiooni aspektid
- M 2.504 Õigusalaste raamtingimuste kontrollimine ja **isikuandme**te töötlemise eelkontroll
- M 2.505 **Isikuandme**te töötlemisega seotud tehniliste-töökorralduslike meetmete kindlaksmääramine vastavalt tehnika tasemele
- M 2.506 Töötajate kohustamine ja koolitamine **isikuandme**te töötlemise alal
- M 2.507 Töökorralduslikud meetmed osapoolte õiguste tagamiseks **isikuandme**te töötlemisel
- M 2.508 Protseduuriloendite haldamine ja teavitamiskohustuste täitmine **isikuandme**te töötlemisel
- M 2.509 **Isikuandme**te kaitse seadusele vastav kasutusse lubamine
- M 2.510 Teabepäringuprotseduuride reeglid **isikuandme**te töötlemisel
- M 2.511 **Isikuandme**te töötlemise tellimustööde reeglid
- M 2.512 Andmete seostamise ja kasutamise reeglid **isikuandme**te töötlemisel
- M 2.513 **Isikuandme**te kaitse nõuetele vastavuse dokumenteerimine
- M 2.514 **Isikuandme**te kaitse tagamine igapäevatöös
- M 2.515 **Isikuandme**te kaitse nõuetele vastav kustutamine ja hävitamine

Lisaks meede M 2.110 Andmeprivaatsuse suunised logimisprotseduurides (leitav: https://iske.ria.ee/8_03//ISKE_kataloogid/7_Kataloog_M/M2/M_2.110)

ISKE ohtude kataloogi andmekaitse osa:

- G 2.61 **Isikuandme**te volitamatu kogumine
- G 2.159 **Isikuandme**te ebapiisav turve veebirakendustes
- G 2.162 **Isikuandme**te töötlemise loa puudumine
- G 2.163 **Isikuandme**te töötlemise sihtotstarbe eiramine
- G 2.164 **Isikuandme**te töötluse õigustatuse põhimõtte eiramine
- G 2.165 Ebapiisav või puuduv tarbetute korduste ja andmete kuhjumise mittevältimine **isikuandme**te töötlemisel
- G 2.166 Andmesaladuse põhimõtte eiramine **isikuandme**te töötlemisel

- G 2.167 Andmesaladuse põhimõtte eiramine **isikuandme**te töötlemisel
- G 2.168 Isikute õiguste rikkumine **isikuandme**te töötlemisel
- G 2.169 Andmetöötlusprotsessi ebapiisav või puuduv kaitse **isikuandme**te töötlemisega seotud tellimustöödes
- G 2.171 Etteantud kontrollieesmärkide ohustamine **isikuandme**te töötlemisel
- G 2.172 Andmetöötlusprotsessi ebapiisav või puuduv kaitse **isikuandme**te töötlemisel välisriikides
- G 2.173 Lubamatud automaatsed otsused üksikjuhtumite kohta **isikuandme**te töötlemisel

ISKE meetmete kataloogi versioonis 8.02. on (https://iske.ria.ee/8_02/ISKE_kataloogid/5_Kataloog_B/B1/B_1.5) andmekaitse moodul B 1.5. suhteliselt lakooniline sisaldades endas üksnes järgmist: „B 1.5 Andmekaitse: Andmekaitse tagamine käesoleva mooduli mõistes tähendab isikuandmete kaitse seaduse järgimist. Andmekaitse Inspektsiooni juhendmaterjalid leiab veebilehelt www.aki.ee, isikuandmete kaitse seadus on leitav Riigi Teatajast. „

ISKE meetmete kataloogi versioonis 7.00 (lisan selle manusena, leitav ka aadressil: https://iske.ria.ee/7_01) on andmekaitse moodul B 1.5. mõnevõrra lahti kirjutatud sisaldades endas meetmeid M 2.501 - M 2.515, mille sisu on järgmine:

B 1.5 Andmekaitse	M 2.501	L	Andmekaitsehaldus
B 1.5 Andmekaitse	M 2.502	L	Andmekaitse vastutusalade kindlaksmääramine
B 1.5 Andmekaitse	M 2.503	L	Andmekaitsekontseptsiooni aspektid
B 1.5 Andmekaitse	M 2.504	L	Õigusalaste raamtingimuste kontrollimine ja isikuandmete töötlemise eelkontroll
B 1.5 Andmekaitse	M 2.505	L	Isikuandmete töötlemisega seotud tehniliste-töökorralduslike meetmete kindlaksmääramine vastavalt tehnika tasemele
B 1.5 Andmekaitse	M 2.506	L	Töötajate kohustamine ja koolitamine isikuandmete töötlemise alal
B 1.5 Andmekaitse	M 2.507	L	Töökorralduslikud meetmed osapoolte õiguste tagamiseks isikuandmete töötlemisel
B 1.5 Andmekaitse	M 2.508	L	Protseduuriloendite haldamine ja teavitamiskohustuste täitmine isikuandmete töötlemisel
B 1.5 Andmekaitse	M 2.509	L	Andmekaitseseadusele vastav kasutusse lubamine
B 1.5 Andmekaitse	M 2.510	L	Teabepäringuprotseduuride reeglid isikuandmete töötlemisel
B 1.5 Andmekaitse	M 2.511	M	Isikuandmete töötlemise tellimustööde reeglid
B 1.5 Andmekaitse	M 2.512	L	Andmete seostamise ja kasutamise reeglid isikuandmete töötlemisel
B 1.5 Andmekaitse	M 2.513	L	Andmekaitsenõuetele vastavuse dokumenteerimine
B 1.5 Andmekaitse	M 2.514	L	Andmekaitse tagamine igapäevatöös
B 1.5 Andmekaitse	M 2.515	L	Andmekaitsenõuetele vastav kustutamine ja hävitamine

Alates 2010. aasta lõpust on algselt JM justiitshalduspoliitika osakonna infosüsteemide ja tööprotsesside talituse (alates 01.08.2015 JM üldosakonna infotehnoloogia ja andmeturbe talituse)

nõunikuna palgal isikuandmete kaitse eest vastutav isik, kelle põhiülesandeks on JM-is ja JM-i haldusalas isikuandmete töötlemise õiguspärasuse tagamine.

Isikuandmete töötlemise õiguspärasuse tagamiseks JM-is ja JM-i haldusalas on vastutav isik juurutanud, rakendanud ning rakendab järjepidevalt kõiki moodulis kirjeldatud isikuandmete kaitse meetmeid ning on rakendanud ka muid meetmeid, mille algatajaks või rakendajaks vastutav isik vastavalt IT Baseline Protection Manual`ile on määratud, näiteks M 2.110 Logimisprotseduuride reeglite kehtestamine.

M 2.110 Logimisprotseduuride reeglite kehtestamine

Algataja: IT juht, DPO[1]
Rakendaja: administraator, DPO

Infosüsteemide haldamise puhul tähendavad logid eelkõige manuaalsete või automatiseeritud kirjete loomist ja säilitamist, mille eesmärgiks on luua võimalused vastamaks küsimusele „Kes on, millal ja milliseid kanaleid kasutades taotlenud või saanud juurdepääsu millistele andmetele?“ Logide loomise ja säilitamise kohustus tuleneb eelkõige isikuandmete kaitse seaduse §-is 25 sätestatud nõuetest, aga ka näiteks etalonturbesüsteemist ISKE.

Minimaalne logimiskohustus

Põhjalik logide säilitamise kohustus peab hõlmama vähemalt alljärgnevaid infosüsteemi haldamisega seonduvaid tegevusi ja toiminguid.

Süsteemi konfiguratsiooni ja süsteemi parameetrite muutmine
Kontode loomine
Õiguste profiilide loomine
Rakendustarkvara installeerimine ja muutmine
Failisüsteemi muutmine
Varundamisoperatsioonid
Haldustarkvara toimingud
Autoriseerimata sisselogimise ja väljastatud õiguste kuritarvitamise katsed
Andmete sisestus
Andmete edastus
Andmetele juurdepääs
Andmete kustutamine
Kõik toimingud

Logifailide eesmärgipärase kasutamise tagamine

Logifaile võib kasutada üksnes sellel eesmärgil, milleks need esialgselt loodi ning milleks neid kogutakse. Eelkõige on logifailide töötlemise ja kasutamise eesmärgiks kontrollida, et andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks. Kontrollifunktsiooni võivad teostada nii asutusesisesed kui ka välised audiitorid, näiteks isikuandmete kaitse järelevalveorgan või asutuse infosüsteemile juurdepääsu omava asutuse sisekontrolliüksus. Logifailide kasutamine muul otstarbel, kui need algselt koguti, on lubatud üksnes väga äärmuslike olukordade puhul (näiteks nende kasutamine kriminaalmenetluses).

Logifailide kustutamise tähtajad

Logifailide kustutamise tähtaegade määratlemisel tuleb lähtuda eelkõige konkreetsest infosüsteemist, seal sisalduvatest andmetest ja nende säilitamise tähtaegadest ning andmete ebaseadusliku töötlemisega seonduvate õigusrikkumiste aegumise tähtaegadest. Üldine logifailide säilitamistähtaeg

[1] DPO – edaspidiselt *isikuandmete kaitse eest vastutava isiku* tähenduses

tuleneb isikuandmete töötleja kohustusest eesmärkide saavutamiseks mittevajalikud isikuandmed viivitamata kustutada või sulgeda.

Juhtnöörideks võivad olla:

- Võimalus ebakorrapärasusi avastada
- Võimalus ebakorrapärasuste põhjuseid logifailide ja muude andmete ja dokumentatsiooni põhjal ja abil tuvastada

Kogemused on näidanud, et logifailide säilitamistähtaegade kehtestamisel ei tohiks säilitustähtaeg ületada ühte aastat.

Tehniline ja organisatsiooniline raamistik

Auditite läbiviimisel sõltub logifailide ja nende tõlgendamise efektiivsus oluliselt tehnilistest ja organisatsioonilistest tingimustest. Selles kontekstis tuleb tähelepanu pöörata järgnevatele aspektidele:

- Koostada tuleks auditeerimisplaan, mis näeks ette logifailide säilitamise ja kontrollimise eesmärgi ning ka kaitsemehhanismid töötajate ja teiste hõlmatud isikute (välised kasutajad) õiguste kaitseks.
- Tagada tuleb logifailide koostamise ja säilitamise kohustuslik, täielik ning terviklik iseloom.
- Efektiivsed turvameetmed logifailide eesmärgipärase töötlemise tagamiseks.
- Logifailid peavad olema struktureeritavad ja kategoriseeritavad viisil, mis võimaldaks nende lihtsat läbivaatamist. See hõlmab ka IT-tuge ja logifailide hõlpsat kättesaadavust.
- Logifailide läbivaatamise meetodid peavad olema eelnevalt kokku lepitud ja defineeritud.
- Logifailide läbivaatused peavad olema korraldatud piisavalt lühikeste ajavahemike järel, et oleks võimalik minimaliseerida ebakorrapärasuste avastamisel nendest tulenevat kahju ja teha järeldusi. Logifailide läbivaatused peaksid toimuma vahetult enne logifailide säilitamistähtaegade saabumist.
- Läbivaatus ja audit peaksid toimuma 4 silma printsiipi järgides (DPO ja infoturbejuht).
- Logifailide läbivaatuste käigus avastatavate rikkumiste tagajärjed peavad olema eelnevalt kirjeldatud ja teada.
- Töötajaid tuleks teavitada korraldatavatest auditidest. Vajadusel võib auditeid läbi viia ka ette teatamata.

Rutiinsel logifailide läbivaatusel tuleks kasutada automatiseeritud logifailide monitoorimise lahendusi (valvekoerad).

M 2.501 Isikuandmete kaitse korraldus

Algataja: asutuse juhtkond
Rakendaja: infoturbe juht, DPO

Isikuandmete kaitse korraldus tähendab erinevaid protsesse, mis on vajalikud tagamaks õigusaktidest tulenevate isikuandmete kaitse nõuete täitmist ja rakendamist isikuandmeid töötlevate ja sisaldavate infosüsteemide kavandamisel, loomisel, kasutamisel ja kasutuse lõpetamisel.

Isikuandmete kaitse protsess
Isikuandmete kaitse korraldus tuumaks on isikuandmete kaitse protsess. Selleks, et oleks võimalik muutuvas keskkonnas õigusaktidest tulenevate isikuandmete kaitse nõuete täitmist ja rakendamist pidevalt tagada, peaks isikuandmete kaitse protsess olema tsükliline nagu ka infoturbe protsess. Protsess hõlmab kohustusi, mis tõusetuvad organisatsiooni strateegilisel, taktikalisel ja töökorralduslikul tasemel. Protsess on struktureeritud viisil, mis võimaldab luua isikuandmete kaitse korralduse süsteemi ka väikestes organisatsioonides, kus inimressursid on piiratud.

Isikuandmete kaitse protsessi algatamine

Isikuandmete kaitse poliitika (privaatsuspoliitika) koostamine

Isikuandmete kaitse haldajate ja rakendajate määramine (DPO)

Isikuandmete kaitse kontseptsiooni loomine

On seotud infoturbepoliitika või -kontseptsiooniga. Isikuandmete kaitse kontseptsiooni koostamisele järgneb *gap* analüüs, selgitamaks välja moodulis kirjeldatud, kuid asutuses veel rakendamata isikuandmete kaitse meetmed.

Puuduvate isikuandmete kaitse meetmete rakendamine
See protsessi faas hõlmab moodulis kirjeldatud, kuid asutuses veel rakendamata isikuandmete kaitse meetmete rakendamist. Rakendamine toimub tavapärase projektijuhtimise teel, koos projekti rakendamise plaani ja täitjatega.

Isikuandmete kaitse käigus hoidmine
Selle protsessi eesmärk on reageerida muutustele ja muudatustele isikuandmeid töötlevate infosüsteemide töös. Nendeks on eelkõige:

- Isikuandmete kaitse alaste õigusaktide muutmine.
- Muutused (IT) protseduurides
- Turvaintsidentidena käsitletavad häired infosüsteemide ja tööprotsesside töös.
- Tehniline areng

Eelmainitud eesmärgi täitmine eeldab teatud alaprotsesside kehtestamise vajadust, mille käigus hallatakse iseseisvalt muutusi ja muudatusi isikuandmete töötlemisega seonduvas. Muudatused või muutused võivad tingida vajaduse muuta isikuandmete kaitse protsessi haldamise struktuuri või isikuandmete kaitse kontseptsiooni uuendamist.

Turvaintsidentide käsitlemine
Infosüsteemides toimunud infoturbeintsidentide käsitlemine peab hõlmama intsidentide põhjuste väljaselgitamist ning nende hindamist isikuandmete kaitse aspektist. See saavutatakse parimal viisil kui infoturbeintsidenti käsitletakse koostöös intsidendi uurimist juhtiva infoturbespetsialistiga. Isikuandmete kaitse halduse rolliks on seejuures:

- Seada prioriteedid tehnilistele ja organisatsioonilistele meetmetele ja nende võimalikule muutmise vajadusele ja probleem lahendada ning isikuandmete kaitse alaste õigusaktide rikkumise kohta tõendusmaterjali kogumine.
- Isikuandmete kaitse alaste õigusaktide rikkumisest tulenevate õiguslike küsimuste lahendamine.

Seega tuleks kõikide isikuandmeid töötlevates infosüsteemides aset leidnud infoturbeintsidentide uurimisse automaatselt kaasata ka isikuandmete kaitse eest vastutav isik.

IT-süsteemide elutsükli haldamine isikuandmete kaitse seisukohast
Järgib ISKE nagu ka BSI tsüklilist kontseptsiooni, et hallata IT-süsteeme ja tooteid kogu nende elutsükli jooksul. IT süsteemide igas faasis tuleb kaaluda erinevate isikuandmete kaitse moodulis B 1.5 kirjeldatud meetmete rakendamist. See hõlmab:

- Planeerimise ja kavandamise faasis meetmete M 2.501 Isikuandmete kaitse korraldus kuni meetmeni M 2.505 Isikuandmete töötlemisel viimase peal tehnilis-organisatsiooniliste meetmete kehtestamine rakendamist
- Planeerimise ja kavandamise rakendamise faasis (tootmisfaasis) meetmete M 2.506 Isikuandmete töötlemises osaleva personali teadlikkuse tõstmine kuni meetmeni M 2.512 Reeglite kehtestamine isikuandmete ristkasutamisele ja edasisele töötlemisele
- Tavapärase süsteemi töös hoidmise käigus meetmeid M 2.513 Dokumentatsiooni haldamine töötlemistoimingu või infosüsteemi heakskiitmise ja töösse lubamise kohta ning meetme M 2.515 Isikuandmete kaitse nõuete kohane infovarade kasutusest kõrvaldamine ja/või hävitamine rakendamist
- Pärast infosüsteemi sulgemist kuni infosüsteemi ja seal sisalduvate andmete hävitamiseni meetme M 2.508 Isikuandmete töötlemisel töötlemistoimingute registreerimine ja registreerimiskohustuse täitmine rakendamist, meetme M 2.110 Logimisprotseduuride reeglite kehtestamine rakendamist ja meetme M 2.515 Isikuandmete kaitse nõuete kohane infovarade kasutusest kõrvaldamine ja/või hävitamine rakendamist.

Infosüsteemi planeerimise ja kavandamise faasis tuleb lisaks eeltoodule kaaluda võimalust kasutada privaatsust suurendavaid tehnoloogiaid (*Privacy Enhancing Technologies* ehk *PET*). PET-id pakuvad tehnoloogilist tuge isikuandmete põhimõtete nagu näiteks minimaalsuse põhimõtte ja kasutuse piiramise põhimõtte, kohaldamisele. PET-ide heaks näiteks on protokoll P3P (*Platform for Privacy Preferences*), pseudonüümide kasutamine, andmebaasis isikut identifitseerivate andmete ja muude

andmete eraldi hoidmist. Samuti programmide automaatteavituse funktsioonid, mis teavitavad näiteks andmete kustutamise tähtaja saabumisest.

Isikuandmete kaitse alaste õigusaktide muutmine
Oluline on jälgida isikuandmete kaitse alaste õigusaktide muutmisi ning hinnata nende võimalikku mõju asutuses toimuvale isikuandmete töötlemisele.

Tehnoloogiliste arengute jälgimine
Koostöös infoturbe haldusega jälgitakse infoturbele ja isikuandmete kaitsele mõju avaldavaid tehnoloogilisi arenguid. Siia hulka kuulub ka ISKE versiooniuuenduste jälgimine ja nendele reageerimine

M 2.502 Rollide ja vastutuse määratlemine isikuandmete kaitse valdkonnas

Algataja: asutuse juhtkond
Rakendaja: asutuse juhtkond

Isikuandmete kaitse on oluline igas valdkonnas ja süsteemides, kus isikuandmeid töödeldakse. Isikuandmete kaitse aspekt tuleb integreerida infoturbe haldamise raamistikku alates isikuandmete töötlemise või isikuandmeid töötleva infosüsteemi planeerimisest kuni selle valmistamiseni. Alles sellisel juhul saab ja on võimalik infosüsteemi isikuandmete kaitse aspektidele tähelepanu pöörata. Juba valminud lahendusi muuta on oluliselt keerulisem kui nende väljatöötamine isikuandmete kaitse reegleid ja nõudeid silmas pidades.

Sobivaimaks lahenduseks on isikuandmete kaitse eest vastutava isiku (*Data Protection Officer DPO*) määramine ja integreerimine infoturbe haldamise raamistikku. Isikuandmete kaitse eest vastutav isik monitoorib sõltumatult asutuses toimuva isikuandmete töötlemise vastavust isikuandmete kaitse reeglitele ja nõuetele. Samuti tegutseb DPO nö vahemehena tööandjast asutuse ja isikuandmete töötlemise õiguspärasuse üle järelevalvet teostava riikliku järelevalveorgani vahel.

Isikuandmete kaitse eest vastutava isiku määramine

Põhiülesanded:
Nõustab asutuse juhtkonda ja töötajaid isikuandmete kaitsega seonduvates küsimustes
Viib läbi omaalgatuslikke kooskõlastatud ja kooskõlastamata auditeid.

Registreerimiskohustused
Koostab ja peab asutuse isikuandmeid sisaldavate infosüsteemide registrit.
Koostab ülevaate kõikidest asutuses isikuandmeid sisaldavatest andmekogudest ja menetlustest, mille käigus isikuandmeid töödeldakse.
Järgib ja peab kinni kõikidest seadusekohastest teavituskohustustest (sealhulgas isikuandmete töötlemise riikliku järelevalveorgani teavitamiskohustusest)
Auditeerib ja kontrollib lepinguliste partnerite poolset isikuandmete töötlemise ja isikuandmete kasutamise õiguspärasust.

Osalus
Osaleb ja on kaasatud isikuandmete töötlemist puudutavate või seda mõjutavate või mõjutada võivate juhendite, soovituste, kasutustingimuste, poliitikate, kordade ja muude osaliselt või täielikult avalikustamisele kuuluvate dokumentide koostamises.
Osaleb ja on kaasatud andmesubjekti isikuandmetele juurdepääsu, parandamise, sulgemise ja kustutamise õigusega seonduvate küsimuste lahendamisel, sellekohase informatsiooni väljastamisel ning sellest teavitamisel.
Osaleb logifailide hindamisel.
Osaleb isikuandmeid töötleva infosüsteemi planeerimises, loomises, kasutusele võtmises, ümberkujundamises, liidestamises.
Osaleb ja on kaasatud infoturvet puudutavate juhendite ja kordade koostamises.

Koolitus ja koostöö
Koolitab asutuse töötajaid isikuandmete kaitsega seonduvas ning sellest tulenevatest reeglitest ja nõuetest.

Koostab ja esitab asutuse juhtkonnale regulaarseid või *ad hoc* valdkonna või infosüsteemi põhiseid aruandeid isikuandmete kaitse reeglite ja nõuete täitmise kohta.
Teeb tihedat koostööd asutuse infoturbe juhiga.
Tegutseb riikliku isikuandmete kaitse järelevalveorgani ja/või asutuseväliste riiklike või eraettevõtete sarnaste funktsioonide, teenistuskohustuste ja ülesannetega töötajate kontaktisikuna.

M 2.503 Isikuandmete kaitse kontseptsiooni (privaatsuspoliitika) elemendid

Algataja: infoturbe juht, DPO
Rakendaja: infoturbe juht, DPO

Esimese sammuna tuleb määratleda ja dokumenteerida üldised asutuses toimuvale isikuandmete töötlemisele kohalduvad nõuded ja reeglid ning hinnata kuidas neid rakendatakse. Isikuandmete töötlemisele kohalduvate reeglite ja nõuete puhul on alati teatud üldised aspektid, millele tuleb isikuandmete kaitse kontekstis tähelepanu pöörata.
Isikuandmete kaitse kontseptsiooni eesmärgiks on ühes kõiki töötlemistoiminguid hõlmavas dokumendis määratleda ja dokumenteerida üldised isikuandmete kaitse regulatsioonist tulenevad õiguslikud aspektid.

Kaaluda tuleks alljärgnevaid aspekte:

- Kõikide töötlemisprotseduuride registreerimine
- Töödeldavate isikuandmete ulatuse ja eesmärgi määratlemine. Kas töödeldakse otsest tuvastamist võimaldavaid andmeid (isikukood, aadress, maksualane teave) või kaudset tuvastamist võimaldavaid andmeid (auto registreerimisnumber, katastriüksuse number)
- Isikuandmete töötlemise õiguslik alus
- Isikuandmete töötlemine üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks
- Isikuandmete erikategooriate (delikaatsed isikuandmed) töötlemise vajaduse hindamine
- Isikuandmete töötlemine üksnes eesmärkide täitmiseks vajalikus ulatuses (minimaalsuse põhimõte)
- Isikuandmete kaitseks rakendamisele kuuluvad ning rakendatud turvameetmed vastavalt ISKE-le, arvestades töödeldavate andmete turvaklassi, versioonide uuendamine, auditite läbiviimine ning veel rakendamata turvameetmete rakendamine
- Automatiseeritud raporteerimise protseduuride erilised aspektid
- Andmetöötlussüsteemi poolt ilma andmesubjekti osaluseta otsuse (edaspidi *automaatne otsus*) tegemise keelamine välja arvatud seadusega ettenähtud erandid (IKS § 17)
- Andmesubjekti õigus saada enda kohta käivaid isikuandmeid; nõuda ebaõigete isikuandmete parandamist; juhul, kui isikuandmete töötlemine ei ole seadusega lubatud, siis isikuandmete sulgemist või kustutamist; õigus esitada kaebusi ja vastuväiteid ning õigus nõuda ebaseadusliku isikuandmete töötlemisega tekitatud kahju hüvitamist
- Isikuandmete töötlemisega seotud õigusrikkumiste ja sellega kaasnevate tagajärgede ennetamine
- Andmete kustutamine
- Logimine
- Eelkontroll
- Isikuandmete kaitse alaste rollide ja vastutuse määratlemine (M 2.502)
- DPO rollide, vastutuse ja tegevuse kirjeldamine ja sellekohase teabe kättesaadavaks tegemine
- Riikliku järelevalveasutuse rollide, vastutuse ja tegevuse kirjeldamine ja sellekohase teabe kättesaadavaks tegemine
- Isikuandmeid töötlevatele alltöövõtjatele lepinguliste kohustuste kehtestamine
- Isikuandmete kolmandatesse (mittepiisava andmekaitse tasemega) riikidesse edastamise hoolikas kaalumine ning võimalusel andmesubjekti õiguste kaitseks täiendavate lepinguliste kohustuste rakendamine (*Safe Harbour*)
- Isikuandmete kaitseks füüsiliste, infotehniliste ja organisatsiooniliste turvameetmete rakendamise kohustus
- Isikuandmete töötlemises osaleva personali poolne isikuandmete kaitset puudutav deklaratsioon ning koolitamine
- Töötlemistoimingu või infosüsteemi eelnev heakskiitmine ja töösse lubamine
- Isikuandmete töötlemisprotseduuride kirjeldamine

- Riikliku andmekaitse järelevalveasutuse teavitamine (vt ka meede M 2.508 Isikuandmete töötlemisel töötlemistoimingute registreerimine ja registreerimiskohustuse täitmine)
- Isikuandmete kaitse eest vastutava isiku määramine ja tema kohustuste määratlemine (vt ka meede M 2.502 Rollide ja vastutuse määratlemine isikuandmete kaitse valdkonnas)

M 2.504 Õigusliku raamistiku määratlemine ning isikuandmete töötlemise eelkontroll

Algataja: infoturbe juht, DPO, infovara omanik
Rakendaja: infoturbe juht, DPO, infovara omanik

Õigusliku raamistiku määratlemisel ning isikuandmete töötlemise eelkontrolli teostamisel tuleb tähelepanu pöörata alljärgnevatele aspektidele:
- Isikuandmete olemasolu määratlemine
- Isikuandmete töötlemise lubatavuse hindamine
- Isikuandmete töötlemise vajaduse hindamine
- Isikuandmete töötlemine üksnes määratletud eesmärgi täitmiseks
- Spetsiifilisel eesmärgil kogutud isikuandmete eesmärgipärane kasutamine
- Eelkontrolli läbiviimine

Isikuandmete töötlemise lubatavus
Enne isikuandmete kogumist, töötlemist või kasutamist tuleb hinnata iga töötlemistoimingu lubatavust, kas toiminguks on vaja andmesubjekti nõusolekut, kas töötlemine toimub andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks või töödeldakse isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks.

Isikuandmete vajadus
Enne isikuandmete kogumise alustamist või selle kavandamise faasis tuleb hinnata, kas isikuandmeid on eesmärgi täitmiseks üleüldse vaja või saab eesmärgi täita ka isikuandmeid kasutamata. Juhul, kui isikuandmete kasutamine osutub eesmärgi täitmiseks hädavajalikuks, tuleb hinnata, kas isikuandmeid kogutakse eesmärgi täitmiseks vajalikus ulatuses ning kas eesmärki ei ole võimalik täita vähemal määral isikuandmeid kogudes.
Sama põhimõtet tuleb rakendada iga asutuse isikuandmetele juurdepääsu vajava töötaja juurdepääsuõiguse andmise otsustamisel, kas konkreetsel asutuse töötajal on tööülesannete täitmiseks hädavajalik isikuandmetele juurdepääs, kas see on vajalik soovitud ulatuses.

Tehnoloogiliste lahenduste valimisel, tuleb eelistada lahendusi ja rakendusi, mis eeldavad isikuandmete võimalikult vähest kasutamist, kogumist, töötlemist. Kohaldub isikuandmete töötlemise minimaalsuse põhimõte – isikuandmeid võib koguda ja töödelda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.

Isikuandmete eesmärgipärane töötlemine
Enne isikuandmete arhiveerimist, muutmist või kasutamist tuleb hinnata kas eelmainitud töötlemistoimingud toimuvad samadel eesmärkidel, millistel isikuandmed algselt koguti või arhiveeriti.
Isikuandmete kasutuse piiramise põhimõtte kohaselt võib isikuandmeid muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal.

Spetsiifilisel eesmärgil kogutud isikuandmete eesmärgipärane kasutamine
Tuleb kindlaks määrata, et spetsiifilisel ja kitsalt piiritletud eesmärgil kogutud isikuandmete, näiteks isikuandmete kaitse auditeerimise eesmärgil kogutud isikuandmeid sisaldavaid logisid kasutatakse üksnes selle kogumise aluseks olnud eesmärgil.

Eelkontrolli läbiviimine
Enne isikuandmeid töötleva infosüsteemi tootmisfaasi saatmist, tuleb läbi viia eelkontroll avastamaks, hindamaks ja määratlemaks riske ja ohte, mida süsteemi kasutuselevõtmine võib andmesubjekti informatsioonilisele enesemääramisõigusele tekitada.
Eelkontrolli käigus tuleb tähelepanu pöörata alljärgnevatele aspektidele:
- Füüsiline juurdepääs isikuandmeid töötlevatele seadmetele
- Süsteemile juurdepääs
- Süsteemis sisalduvatele andmetele juurdepääs

- Andmete edastamine
- Andmete sisestamine
- Lepingulised suhted kolmandate isikutega
- Käideldavus
- Erinev töötlemine erinevatel eesmärkidel kogutud isikuandmete suhtes.

Rakendatavad turvameetmed peavad vastama süsteemis sisalduvatele isikuandmete tasemele. Juhul kui isikuandmeid ei töödelda automatiseeritult, tuleb tagada, et andmekandjate arhiveerimisel, hoidmisel, transportimisel ja hävitamisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist.

M 2.505 Isikuandmete töötlemisel viimase peal tehniliste-organisatsiooniliste meetmete kehtestamine

Algataja: asutuse juhtkond, infoturbe juht, DPO
Rakendaja: infovara omanik, infoturbe juht, DPO

Isikuandmete töötleja on kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks:
1) andmete tervikluse osas – juhusliku või tahtliku volitamata muutmise eest;
2) andmete käideldavuse osas – juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest;
3) andmete konfidentsiaalsuse osas – volitamata töötlemise eest.

Isikuandmete töötleja on isikuandmete töötlemisel kohustatud:
1) vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele;
2) ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis, samuti andmekandjate omavolilist teisaldamist;
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;
4) tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks;
5) tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise;
6) tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist;
7) kujundama ettevõtte, asutuse või ühenduse töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid.

Turvameetmete valik sõltub suuresti töödeldavatest andmetest ning peab vastama vastavale ISKE turvaklassile. Eelmainitud turvameetmete rakendamise kohustus tuleb lisada asutuse infoturbe ja isikuandmete kaitse alastesse regulatsioonidesse.

M 2.506 Isikuandmete töötlemises osaleva personali teadlikkuse tõstmine

Algataja: asutuse juhtkond
Rakendaja: DPO, personaliosakond, otsesed juhid

Vajadusel tuleb asutuse uutel töötajatel allkirjastada isikuandmete kaitse alane deklaratsioon, millega võetakse kohustus töödelda isikuandmeid üksnes õiguspärastel ning tööülesannetest tulenevatel eesmärkidel. Samuti kohustus hoida teatavaks saanud isikuandmeid saladuses ka pärast töösuhte lõppu. Kindlasti tuleb tähelepanu pöörata ka asutuse töötajate isikuandmete kaitse alase teadlikkuse tõstmisele, kas vastavate koolituste korraldamisega või juhendite koostamisega.

M 2.507 Andmesubjekti õiguste kaitseks organisatsiooniliste reeglite kehtestamine

Algataja: Infovara omanik, DPO
Rakendaja: Infovara omanik, DPO

Tuleb rakendada tehnilis-organisatsioonilisi meetmeid, et andmesubjekt saaks oma õigust saada enda kohta käivaid isikuandmeid; õigust saada enda kohta käivate andmete töötlemisega seonduvate teavet (sealhulgas teavet, kellele on tema isikuandmeid edastatud) õigust nõuda ebaõigete isikuandmete parandamist; juhul, kui isikuandmete töötlemine ei ole seadusega lubatud, siis õigust nõuda isikuandmete sulgemist või kustutamist; õigust esitada kaebusi ja vastuväiteid ning õigust nõuda ebaseadusliku isikuandmete töötlemisega tekitatud kahju hüvitamist, hõlpsasti ja lihtsalt realiseerida. Võimaluse korral tuleks eelistada eelmainitud õiguste realiseerimise infotehnoloogilisi lahendusi.

M 2.508 Isikuandmete töötlemisel töötlemistoimingute registreerimine ja registreerimiskohustuse täitmine

Algataja: IT juht, DPO
Rakendaja: Infovara omanik, DPO

Meede hõlmab endast kõikide isikuandmete kaitse alaste õigusaktidega kehtestatud isikuandmete töötlemisega seonduvate registreerimiskohustuste täitmist. Isikuandmete kaitse eest vastutav isik on kohustatud pidama asutuse andmetöötlemise registrit, mille eesmärgiks on koondada ühtsesse registrisse koondandmestikud asutuse erinevate registrite, andmekogude ja infosüsteemide kohta, milles töödeldakse delikaatseid isikuandmeid. Register sisaldab asutuse delikaatseid isikuandmeid sisaldavate registrite, andmekogude ja infosüsteemide, mille vastutavaks töötlejaks asutus on, kohta vähemalt alljärgnevad andmed:
1) isikuandmete töötleja, sealhulgas volitatud töötleja nimi, registri- või isikukood, tegevuskoht, asu- või elukoht ja muud kontaktandmed;
2) viide isikuandmete töötlemise õiguslikule alusele;
3) isikuandmete töötlemise eesmärgid;
4) isikuandmete koosseis;
5) isikute kategooriad, kelle andmeid töödeldakse;
6) isikuandmete allikad;
7) isikud või nende kategooriad, kellele isikuandmete edastamine on lubatud.

Lisaks eeltoodule on isikuandmete töötleja kohustatud pidama arvestust isikuandmete töötlemisel kasutatavate tema kontrolli all olevate seadmete ja tarkvara üle, dokumenteerides järgmised andmed:
1) seadme nimetus, tüüp ja asukoht ning seadme valmistaja nimi;
2) tarkvara nimetus, versioon, valmistaja nimi ja kontaktandmed.

M 2.509 Töötlemistoimingu või infosüsteemi heakskiitmine ja töösse lubamine

Algataja: asutuse juhtkond, DPO
Rakendaja: asutuse juhtkond

Isikuandmete töötlemisel kasutatavat tarkvara ja infosüsteeme testitakse enne nende tööle rakendamist. Reeglina toimub see testandmetega ning ilma reaalseid isikuandmeid kasutamata. Samas tehakse koormusteste ka reaalsete, kuid identifitseerivatest andmetest puhastatud andmetega. Tuleb kehtestada tarkvara ja infosüsteemide testimise põhimõtted, milliseid andmeid võidakse, millistel tingimustel ja kelle poolt testimisel kasutada.

M 2.510 Isikuandmetele juurdepääsu võimaldamisel kolmandale isikule teatud registreerimis- ja raporteerimisprotseduuride kehtestamine

Algataja: IT juht, DPO
Rakendaja: infovara omanik, DPO

Isikuandmetele juurdepääsu võimaldamine kolmandatele isikutele on isikuandmete kaitse ja isikuandmete turvalisuse aspektist olulise tähtsusega, sõltudes viisist, mil moel isikuandmetele juurdepääsu võimaldatakse. Üldiselt on isikuandmete kaitse seaduse § 14 lõige 2 punkti 1 kohaselt andmesubjekti nõusolekuta tema isikuandmete edastamine või nendele juurdepääsu võimaldamine kolmandale isikule lubatud kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks. Lisaks peab isikuandmete töötleja isikuandmetele kolmandatele isikutele

juurdepääsu võimaldamisel tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks; tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise ning tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist (isikuandmete kaitse seadus § 25 lõige 2 punktid 4, 5 ja 6).

Üldised aspektid:

- Isikuandmetele kolmandatele isikutele juurdepääsu võimaldamise eesmärgi ja kolmandate isikute ringi täpsustamine
- Isikuandmetele juurdepääsuõiguste täpsustamine ja auditeerimine
- Kättesaadavaks tehtavate isikuandmete iseloomu ja juurdepääsu ulatuse täpsustamine
- Juurdepääsuõiguse blokeerimine ja juurdepääsetavate isikuandmete säilitamise tähtaegade täpsustamine
- Kolmanda isiku poolse vastutava töötleja teavitamiskohustuse määratlemine ja täpsustamine
-

Meetmed volitamata juurdepääsu takistamiseks

- Sobivate meetmete rakendamine isikuandmetele juurdepääs tagamiseks üksnes kolmanda isiku autoriseeritud töötajate poolt
- Kasutajakonto blokeerimine peale teatud arvu ebaõnnestunud sisselogimiskatseid
- Salasõna regulaarne vahetamine teatud intervallide möödumisel. Juhul, kui see on tehniliselt võimalik tuleb salasõna vahetuse nõue tagada infotehnoloogiliste vahenditega
- Juurdepääsu delikaatsetele isikuandmetele tuleb kaitsta tugevamate turvameetmetega (multifaktoriline autentimine – ID kaart)
- Logifailide analüüsimiseks tuleb kasutada automatiseeritud auditeerimissüsteeme
- Täpsustada logimise viisi ja ulatust
- Rakendada juhuslikku auditeerimist ja pidevat logimist
- Täpsustada, kas logimiskohustus kohaldub üksnes vastutava töötleja või kolmanda isiku või mõlema juures
- Logide loomisel tuleb arvestada, et need võimaldaksid tagantjärele kindaks teha, kelle juurdepääsuõigusi juurdepääsul kasutati
- Logisid tuleb säilitada isikuandmetele juurdepääsu eesmärgi kohta
- Peale juurdepääsu toimumist, tuleks säilitada logid juurdepääsuviisi ja juurdepääsul kasutatud seadmete kohta

Võrguühendus

Infosüsteemide ühendamisel tuleb tähelepanu pöörata infosüsteemide ühendamise viisile ning sellest lähtuvalt rakendada sobivaid turvameetmeid. Sissehelistamise (*dial-up*) ühenduse puhul tuleb hoolikalt kaaluda sobivate turvameetmete rakendamist, VPN ühenduse puhul tuleb luua kinnised kasutajate grupid. LAN ühenduse puhul tuleb kinnised kasutajate grupid luua viisil, mis võimaldaksid neil kasutada üksnes oma struktuuriüksuse ressursse.

M 2.511 Regulatsioonide kehtestamine alltöövõtulepingute sõlmimisele

Algataja: IT juht, DPO
Rakendaja: infovara omanik, DPO

Juhul, kui isikuandmete töötlemisse kaasatakse lepinguline teenuse pakkuja (volitatud töötleja), siis jääb isikuandmete vastutavaks töötlejaks ikkagi algne isikuandmeid töötlev asutus. Vastutav töötleja annab volitatud töötlejale kohustuslikke juhiseid isikuandmete töötlemiseks ja vastutab selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. Eelmainitud nõuded määrab volitatud töötleja jaoks kindlaks vastutav töötleja.

Volitatud töötleja võib isikuandmete töötlemist edasi volitada üksnes vastutava töötleja kirjalikul nõusolekul ning tingimusel, et ei ületata volitatud töötleja volituste mahtu.

Isikuandmete töötlemiseks on vastutav töötleja kohustatud sõlmima volitatud töötlejaga kirjaliku lepingu, milles järgitakse isikuandmete kaitse alaste õigusaktide nõudeid ning nähakse ette poolte vastutus lepinguliste kohustuste täitmata jätmise eest.

Lepinguga tuleb kindlaks määrata:

- isikuandmete töötlemise eesmärgid;
- töödeldavate isikuandmete koosseis;
- isikuandmete töötlemise kord ja viisid, sealhulgas käesolev isikuandmete kaitseks rakendatavate organisatsiooniliste, infotehniliste ja füüsiliste turvameetmete kirjeldus;
- isikuandmete kolmandatele isikutele edastamise lubatavus.

Volitatud töötleja on kohustatud:

- isikuandmeid töötlema ainult lepingus määratud eesmärgil, korras, viisil ja tingimustel;
- kasutusele võtma ettenähtud isikuandmete organisatsioonilised, füüsilised ja infotehnilised turvameetmed.

Volitatud töötlejal on keelatud kolmandatele isikutele lepinguväliselt üle anda lepingu täitmiseks töödeldavaid isikuandmeid, välja arvatud juhud, kui selleks on vastutava töötleja kirjalik nõusolek või üleandmise kohustus on ette nähtud seadusega.

Füüsiline isik, kes isikuandmete töötleja alluvuses töötleb isikuandmeid, on kohustatud neid töötlema isikuandmete kaitse alaste õigusaktidega lubatud eesmärkidel ja tingimustel ning vastutava töötleja antud juhiste ja korralduste kohaselt ning on kohustatud hoidma saladuses talle tööülesannete täitmisel teatavaks saanud isikuandmeid ka pärast töötlemisega seotud tööülesannete täitmist või töö- või teenistussuhte lõppemist.

Volitav asutus ja DPO võivad eelmainitud nõuete täitmist volitatud töötleja poolt alati inspekteerida.

M 2.512 Reeglite kehtestamine isikuandmete ristkasutamisele ja edasisele töötlemisele

Algataja: IT juht, DPO
Rakendaja: infovara omanik, DPO

Tüüpilise IT rakenduse puhul on kasutaja andmebaasis navigeerimine piiratud erinevate rippmenüüde ja väljadega, mille täitmisel võimaldatakse juurdepääs üksnes vastavalt isikuandmete kaitse reeglitele ja nõuetele eelnevalt kindlaks määratud ja piiratud hulgale andmetele. Ülejäänud päringuid ei täideta. Probleem eksisteerib teatud andmebaasi protokollidega („*free query languages*“) ja ka tavalise kontoritarkvaraga, mille kasutamine ei ole erinevate rippmenüüde ja väljade ning eeldefineeritud päringute-vastustega piiratud, võimaldades pääseda ligi andmetele, millele juurdepääs ei pruugi olla õiguspärane ning lubatud.

Võimalus kasutada isikuandmete töötlemiseks tavalist kontoritarkvara või vaba päringuga andmebaasi protokolli, tuleb piirata nii palju kui võimalik.

M 2.513 Dokumentatsiooni haldamine töötlemistoimingu või infosüsteemi heakskiitmise ja töösse lubamise kohta

Algataja: IT juht, DPO
Rakendaja: infovara omanik

Isikuandmete töötlemiseks kasutusele võetavat riist- ja tarkvara tuleb enne kasutusele võtmist isikuandmete kaitse aspektist hinnata. Hindamise tulemused tuleb dokumenteerida. DPOd tuleb uue infosüsteemi või rakenduse kasutusele võtmise plaanidest ja kavatsustest teavitada juba planeerimisstaadiumis, kuna planeerimisstaadiumis on isikuandmete kaitse alaste õigusaktide võimalike rikkumiste korral, hõlpsam ja kindlasti ka odavam plaane muuta kui hakata pärast muutma juba valmis infosüsteemi.

M 2.514 Isikuandmete kaitse käigus hoidmine

Algataja: asutuse juhtkond
Rakendaja: Infoturbe osakond, infoturbe eest vastutav isik, DPO

Lisaks isikuandmete kaitse eest vastutava isiku määramisele on isikuandmete kaitse aspektist oluliseks meetmeks ka asutuse siseste isikuandmete kaitse auditite läbi viimine. See aitab tagada turvalisust ja isikuandmete kaitse alaste õigusaktide nõuetest kinni pidamist. IT auditi funktsiooni täitja kontrollib teabe

töötluse korrektsust eelkõige infoturbe kontseptsioonist lähtudes. See hõlmab infosüsteemide dokumentatsiooni kontrollimist, infosüsteemile kohalduvate turvameetmete ja ka üldiste turvameetmete rakendamise kontrollimist.

Asutusesisene isikuandmete kaitse auditi funktsioon kuulub tavaliselt isikuandmete kaitse eest vastutava isiku (DPO) töökohustuste hulka (vt meede M 2.502 Rollide ja vastutuse määratlemine isikuandmete kaitse valdkonnas), kes kontrollib isikuandmete töötlemise vastavust isikuandmete kaitse alastest õigusaktidest tulenevatele nõuetele. See hõlmab:

- infosüsteemide kontrollimist õigusliku aluse ja eesmärgipärase töötlemise aspektist
- andmesubjekti õiguste tagamine
- asutuse töötajate isikuandmete kaitse alane koolitamine ja nõustamine
- registreerimiskohustuse täitmine ning IT süsteemide, komponentide ja rakenduste kontrollimine
- tehnilis-organisatsiooniliste turvameetmete rakendamise kohustuste täitmist, tagamaks füüsilist juurdepääsu kontrolli, rollipõhiste juurdepääsuõiguste andmist, andmete turvalist edastamist ja andmete edastamise kohta käivate andmete säilitamist (*audit trail*), kasutajate tegevuse auditeerimist, kontrollmeetmete rakendamist volitatud lepinguliste töötlejate tegevusele ja nende kontrollimist, käideldavusmeetmete rakendamist, kontrolli, et eesmärkide poolest erinev isikuandmete töötlemine toimub eraldi.

IT audit ja isikuandmete kaitse audit tuleks läbi viia koos ning need täiendavad teineteist. Regulaarne logifailide läbivaatamine suurendab potentsiaalsete isikuandmete väärkasutamise juhtumite avastamist tunduvalt.

M 2.515 Isikuandmete kaitse nõuetekohane infovarade kasutusest kõrvaldamine ja/või hävitamine

Algataja: asutuse juhtkond
Rakendaja: Infoturbe osakond, infoturbe eest vastutav isik, DPO

Magnetkandjatel oleva teabe turvaline kustutamine

Nii isikuandmete kaitse kui ka infoturbe seisukohast tuleb tagada, et delikaatse või sensitiivse teabe kustutamisel magnetkandjatelt, oleks kustutamine turvaline s.o. täielik ja pöördumatu. Tavalised „kustuta“ käsud ei ole tavaliselt piisavad, kuna kustutatud teavet on lihtne sobivate programmidega taastada. Teave, mis tuleb turvaliselt kustutada tuleb kustutada, kas teabekandja muutmisel loetamatuks füüsiliste vahenditega (termiline või mehaaniline hävitamine, demagnetiseerimine) või korduva ülekirjutamise teel. Samuti tuleb turvalisel kustutamisel tähelepanu pöörata andmete käitlemise ja säilitamise erinevatele aspektidele, nagu varukoopiad, ajutised või alatised *offline* failid, mis luuakse automaatselt süsteemi poolt või individuaalsete rakenduste või siis osade andmebaasisüsteemide „päevikute“ (*journals*) poolt.
Isikuandmete kaitse aspektist on soovituslik:

- Andmete turvalise kustutamise probleemistik eeldab vastutavate otsusetegijate, administraatorite, infoturbeinimeste ja DPO, aga ka iga kasutaja, teadlikkust. See saavutatakse sobiva instrueerimise ja teavitamise teel.
- Konkreetsel töökohal, tuleb andmete turvalise kustutamise tagamiseks rakendada tehnilis-organisatsioonilisi turvameetmeid. Need tuleb integreerida organisatsiooni üldisesse turbe ja isikuandmete kaitse kontseptsiooni. Eelkõige tuleb täpsustada ja määratleda turvameetmed, mis tuleb rakendada enne andmete meediumi müümist, rentimist, kasutusest kõrvaldamist, tagastamist, parandamist või hooldamist.
- Andmete turvalise kustutamise meetmed tuleb lisada konkreetsetele andmete töötlus protseduuridele. Need meetmed peavad olema proportsioonis vastavale andmete kategooriale kohalduvate nõuetega, nagu ka kustutatavate andmete võimalikule taastamisele kuluva pingutuse ja kuluga.
- Säilitamisväärtusega teavet tuleks säilitada võimaluse korral meediumil krüpteerituna. Selleks tuleb kasutada krüpteerimisvõimelisi failisüsteeme. Sarnaselt tuleb krüpteerimisvõimelisi failisüsteeme kasutada ajutiste ja *offline* failide, nagu ka varukoopiate tegemiseks, kuna ka need sisaldavad kaitstavat teavet.
- Terviklikel säilitusmeediumitel (*intact storage media*) olevat teavet saab turvaliselt kustutada ühe- või mitmekordse ülekirjutamise teel suvaliselt valitud teabega. Selleks saab kasutada

spetsiaalset tarkvara (näiteks BSI poolt üllitatud VS Clean). Üldiste ülekirjutamismallide (*uniform overwriting patterns*) kasutamist andmete turvaliseks kustutamiseks tuleks vältida, kuna need ei paku kaitset tõhusate laboratooriumi analüüside abil andmete taastamise eest.
- Tavaliste andmete turvaliseks kustutamiseks võib kasutada andmete ühekordset ülekirjutamist. Isikuandmete puhul peaks andmete ülekirjutamise protsess koosnema vähemalt kahest, veelgi parem kolmest ülekirjutamise korrast. Teisel korral kasutatav ülekirjutamismuster (bitijada) peaks olema täiendav esimesele korrale. Kolmandal korral soovitakse kasutada juhuslikke andmeid. Sel moel saavutatakse kõrgem kaitse tase.
- Juhul kui terviklik andmekandja müüakse, renditakse, kõrvaldatakse kasutusest, tagastatakse või kasutatakse muul otstarbel, tuleks see enne mitmekordselt kasutades juhuslikke andmeid üle kirjutada. Selliselt talitades on võimalik meediumi teistel eesmärkidel taaskasutada (näiteks operatsioonisüsteemi uuesti installeerides).
- Üksikute failide selektiivne kustutamine on üldjuhul problemaatiline. See on sobilik üksnes juhul, kui on ilmselge, et failist ei eksisteeri mujal asuvaid koopiaid (ajutised failid, *offline* mälu või tagavara koopia) või juhul, kui eelmainitud mujal asuvad koopiad suudetakse täpselt määratleda ning samuti turvaliselt kustutada. Veenduda tuleb, et juhul kui sensitiivset teavet sisaldavad ka metaandmed, tuleb ka need turvaliselt kustutada.
- Valides andmete ülekirjutamise teel kustutamiseks tehnilis-organisatsioonilisi turvameetmeid ja töötlemistoiminguid, tuleks tarkvara valikul arvestada kasutajate hinnanguid. Samuti tuleks sellist tarkvara juhuvalikuga testida.
- Kahjustatud säilitusmeedium, millel olevat teavet ei ole võimalik tarkvaraliselt üle kirjutada, tuleb muuta kasutamatuks kas füüsilise või termilise töötlusega (disketid, kõvakettad) või demagnetiseerides (disketid, magnetilised kõvakettad).

Juhul, kui tekib vajadus andmete säilitamiseks kasutatavate seadmete kontrollitud keskkonnast välja viimiseks ilma nendel sisalduvaid andmeid kustutamata (näiteks parandus, garantiiremont), tuleb kasutada vastavaid lepingulisi tingimusi ning vajadusel kahju hüvitamise kohustust soovimatu konfidentsiaalsuskao ilmnemisel, proportsioonis andmete sensitiivsuse tasemega. Juhul, kui see ei ole võimalik, siis tuleb selliseid teenuseid garantii kontekstis mitte kasutada.

Paberkandjate hävitamine

Kuna paberkandjate hävitamine toimub tavaliselt mitmes etapis, tuleb kõikides etappides infoturbe aspektidele tähelepanu pöörata, alates paberkandjate ajutisest säilitamisest prügi- või kogumiskastides, nende kokku kogumise, transpordi ja füüsilise hävitamise protsessini.

Üldised nõuded

Juhul, kui isikuandmeid töödeldakse manuaalselt paberkandjal, tuleb eelkõige rakendada meetmeid vältimaks kõrvaliste isikute ligipääsu paberkandjatele nii nende töötlemise, transpordi kui ka hävitamise etapis. Põhimõtteliselt on isikuandmete vastutav töötleja vastutav paberkandajal olevate isikuandmete kaitse meetmete eest kuni kandjate füüsilise hävitamiseni. Seega peab vastutav töötleja kuni nende füüsilise hävitamiseni omama kontrolli kõikide isikuandmeid sisaldavate paberkandjate üle. Eelkõige ei tohi sellised kandjad enne hävitamist sattuda kõrvaliste ja asjasse puutumatute isikute valdusesse. Määratleda tuleb, millal loetakse paberkandja hävitatuks. Juhtnööriks võib kasutada DIN standardit 32757 (andmekandjate hävitamine). Selle kohaselt loetakse andmekandja hävitamine piisavaks, kui säilitusmeedium on hävitatud selliselt, et seal säilitatud andmete reprodutseerimine või taastamine on võimalik üksnes väga suure pingutuse, inimressursi, vahendite või ajaga (turbeaste 3).

Isegi paberkandjate hävitamisel peab vastutav organisatsioon regulaarselt korraldama auditeid kontrollimaks, et hävitamist teostatakse korrektselt. See on eriti oluline, kui hävitamist teostab alltöövõtu korras organisatsioonivälise teenuse pakkuja. Isikuandmete vastutav töötleja peab sellisel juhul olema täielikult kursis hävitamise protseduuri tehniliste ja organisatsiooniliste iseärasustega, alates paberkandjate üleandmisest teenuse pakkujale kuni paberkandjate füüsilise hävitamiseni, hõlmates endas ka turvalist transporti. Vastutav töötleja peab organisatsioonisiseselt määrama isiku, kes paberkandjate hävitamist auditeeriks.

Paberkandjate hävitamine majasiseselt

Kõige tähtsamaks põhimõtteks peaks olema hävitada paberkandjad nii kiiresti kui võimalik sama organisatsiooni poolt, kes otsustab need ringlusest kõrvaldada. Vahepealne hoiustamine ning

edastamine osapoolelt osapoolele, on väga riskantne ning eeldab rangeid reegleid ning kontrollimist. Paberkandja kohene hävitamine organisatsiooni enese poolt on seega sobivaimaks lahenduseks. Selleks tuleb aga igal juhul kehtestada reeglid, kuidas ringlusest kõrvaldamisele kuuluvaid paberkandjaid hävitada. Paralleelselt peavad nad kuni kandja hävitamiseni olema kohustatud kandjat turvaliselt hoiustama.

Juhul, kui paberkandjaid hävitatakse tsentraalselt, peab kogu hävitamise protsess olema kirjalikult reguleeritud. See kehtib eriti paberkandjate turvalise kokku kogumise ja nende hävitamise kohta transportimisel. Dokumentide turvalisus tuleb tagada ka hävitamisele kuuluvate dokumentide kogumiskohta edastamisel. Juhul, kui hävitamisele kuuluvad dokumendid kogutakse kokku organisatsioonivälise teenuse pakkuja poolt, tuleb selle staadiumi turvalisuse aspektid hoolikalt läbi kaaluda. Dokumentide reaalne hävitamine tuleb sobival viisil registreerida.

Paberkandjate hävitamine organisatsioonivälise teenuse pakkujate poolt.
Juhul, kui paberkandjad kuuluvad hävitamisele organisatsioonivälise volitatud töötlejast teenuse pakkuja poolt, peab kogu dokumentide käitlemise ja nende turvalisuse tagamise protsess, alates nende üleandmisest kuni hävitamise lõpetamiseni olema teenuse pakkujaga sõlmitavas lepingus määratletud.

Dokumentide transport, nende vahepealne vajaduse korral toimuv hoiustamine, hävitamispunkti asukoht, nagu ka maksimaalne viiteaeg dokumentide üleandmise ja lõpliku hävitamise vahel, tuleb kindlaks määrata. Samuti tuleb kirjalikult määratleda, millisel kujul peavad dokumendid olema, et lugeda need hävitatuks. Teenuse pakkuja peab välistama volitamata isikute ligipääsu hävitamisele kuuluvatele dokumentidele. Hävitamisele kuuluvate dokumentide teenuse pakkujale üleandmine tuleb registreerida ning lõpliku hävitamise kohta peab teenuse pakkuja andma oma kirjaliku kinnituse. Üldiselt tuleb vältida hävitamise alltöövõtu korras edasivolitamist teenuse pakkuja poolt.

Vastutav töötleja peab omama täielikku juurdepääsu enda vastutusel olevatele ning hävitamisele kuuluvatele dokumentidele kuni nende lõpliku hävitamiseni. Seega peavad dokumendid kuni hävitamiseni olema vastutava töötleja kontrolli all. Seetõttu ei tohi neid kuni hävitamiseni segada teistelt organisatsioonidelt pärinevate hävitamisele kuuluvate dokumentidega. Teenuse pakkujaga tuleb kokku leppida, et isikuandmete vastutaval töötlejal ja selle isikuandmete kaitse eest vastutaval isikul (DPO) on õigus kuni dokumentide hävitamiseni kogu protsessi auditeerida.

Mis puudutab isikuandmete töötlemise või teatud töötlemistoimingute edasivolitamist organisatsioonivälisele teenuse pakkujale, tuleb viidata meetmele M 2.511. **Regulatsioonide kehtestamine alltöövõtulepingute sõlmimisele.**