Isikuandmete kaitse seaduse eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

25. maist 2018 hakkab isikuandmete kaitse õigust reguleerima otsekohalduv Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta[1] (*üldmäärus*), mis tingib ka vajaduse praegu kehtiv riigisisene regulatsioon üle vaadata.

Seni on isikuandmete kaitse õiguse küsimusi reguleerinud üldseadusena isikuandmete kaitse seadus (kehtiv *IKS*), millega on üle võetud direktiiv 95/46/EÜ, mis aga tunnistatakse 25. maist 2018 kehtetuks.

Kuigi üldmääruse puhul on tegemist EL-i otsekohalduva õigusaktiga, on teatud küsimustes jäetud liikmesriikidele kaalutlusõigus riigisiseselt täpsustada, kehtestada ja säilitada üldmääruses sätestatud isikuandmete töötlemisega seotud küsimusi.

Isikuandmete kaitse õiguses on alates 25. maist 2018 keskne roll üldmäärusel. Eesti õigusakt, uus IKS, loob üldised raamid isikuandmete töötlemisele, milles meil on üldmäärusest tulenev diskretsioon. Samuti võetakse uue IKS-iga üle Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK[2] (*õiguskaitseasutuste direktiiv*).

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud justiitsministeeriumi õiguspoliitika osakonna avaliku õiguse talituse nõunik Sandra Mikli (Sandra.Mikli@just.ee, 620 8245), justiitsministeeriumi kriminaalpoliitika osakonna karistusõiguse ja menetluse talituse nõunik justiitsküsimustes Eesti Vabariigi alalises esinduses EL-i juures (Julia.Antonova@mfa.ee, +32 2227 3916), justiitsministeeriumi õiguspoliitika osakonna avaliku õiguse talituse nõunik Katariina Kärsten (Katariina.Karsten@just.ee, 620 8177, käesoleval ajal õiguskorralduse talituse nõunik), avaliku õiguse talituse juhataja Illimar Pärnamägi (Illimar.parnamagi@just.ee, 620 8175). Varem on eelnõu koostamisega tegelenud Merike Kaev ning Liis Piilberg (mõlemad teenistusest lahkunud).

---

[1] 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: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679.

[2] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:32016L0680.

Mõjude osa on koostanud justiitsministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse nõunik Pilleriin Lindsalu (Pilleriin.Lindsalu@just.ee, 620 8221). Eelnõu keeletoimetaja on justiitsministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Taima Kiisverk (Taima.Kiisverk@just.ee, 620 8181).

1.3. Märkused

9. mail 2017 saadeti ministeeriumidele kooskõlastamiseks ning huvirühmadele arvamuse avaldamiseks „Isikuandmete kaitse uue õigusliku raamistiku“ kontseptsioon. Kontseptsiooni kohta esitatud seisukohti on võetud arvesse ka uue isikuandmete kaitse seaduse eelnõu koostamisel.

Eelnõu seadusena vastuvõtmiseks on vajalik Riigikogu poolthäälte enamus, kuna põhiseaduse § 73 kohaselt võetakse Riigikogu aktid vastu poolthäälte enamusega. Eelnõu on seotud õiguskaitseasutuste direktiivi ülevõtmise ning üldmääruses sätestatud küsimuste täpsustamise ja täiendamisega ulatuses, milles liikmeriikidele on see õigus antud.

2. Seaduse eesmärk

Füüsiliste isikute kaitse isikuandmete töötlemisel on põhiõigus. Euroopa Liidu põhiõiguste harta[3] (*harta*) artikli 8 lõikes 1 ja Euroopa Liidu toimimise lepingu[4] (*EL-i toimimise leping*) artikli 16 lõikes 1 on sätestatud, et igaühel on õigus oma isikuandmete kaitsele. Üldmääruse eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel põhineva majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, Euroopa Liidu majanduse tugevdamisele ja lähendamisele ning füüsiliste isikute heaolule.

Kiire tehnoloogiline areng ja üleilmastumine on tekitanud isikuandmete kaitsel uusi väljakutseid. Isikuandmete kogumise ja jagamise ulatus on märkimisväärselt suurenenud. Tehnoloogia võimaldab nii eraõiguslikul juriidilisel isikul kui ka avaliku võimu kandjal kasutada isikuandmeid oma tegevuses enneolematus ulatuses. Euroopa Komisjon on väljendanud seisukohta, et andmekaitsereegleid on vaja põhjalikult reformida, et tugevdada õigust eraelu puutumatusele internetis ja elavdada Euroopa digitaalmajandust.

Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ[5], mille on üle võtnud ka praegu kehtiv IKS, ei ole ära hoidnud Euroopa Liidus (*EL*) andmekaitse rakendamise killustumist ega õiguskindlusetust, mille tõttu tegi Euroopa Komisjon ka 2012. aastal ettepaneku ajakohastada 1995. aasta andmekaitsedirektiivi põhimõtteid, et tagada edaspidigi õigus eraelu puutumatusele.

---

[3] Euroopa Liidu põhiõiguste harta: http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:et:PDF.

[4] Euroopa Liidu toimimise leping: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:C2010/083/01&from=EN

[5] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta: http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:31995L0046.

Ettepanekud hõlmasid kahte õigusakti:
1. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi ka *üldmäärus*).
2. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (edaspidi ka *õiguskaitseasutuste direktiiv*).

Üldmäärust hakatakse kohaldama alates 25. maist 2018 ning see on tervikuna siduv ja vahetult kohaldatav kõikides EL-i liikmesriikides. Üldmääruse eesmärgiks on ajakohastada kehtivad andmekaitsereeglid, võttes arvesse majanduse digiteerimist, uute tehnoloogiate kasutuselevõttu ning piiriüleste tehingute arvu kasvu. Uute tehnoloogiate kasutuselevõtu kohta on üldmääruse põhjenduspunktis 15 öeldud, et füüsiliste isikute kaitse peaks olema tehnoloogiliselt neutraalne ega tohiks sõltuda kasutatud meetoditest.

Praegu reguleerib isikuandmete kaitse õigust üldseadusena IKS (kehtiv IKS), millega on üle võetud direktiiv 95/46/EÜ. Alates 25. maist 2018 tunnistatakse direktiiv 95/46/EÜ kehtetuks, mida asendab otsekohalduv üldmäärus. Kuna kehtiva IKS-iga on üle võetud direktiiv, mis tunnistatakse kehtetuks, siis tuleb riigisiseselt tunnistada kehtetuks ka kehtiv IKS. Alates 25. maist 2018 reguleerivad isikuandmete kaitse õigust Eestis kui EL-i liikmesriigis otsekohalduv üldmäärus ning uus IKS, milles täpsustatakse ja täiendatakse üldmääruse küsimusi ulatuses, milles liikmesriikidele on see õigus antud.

Euroopa Komisjon on üldmääruse ja direktiivi väljatöötamise käigus defineerinud kolm peamist probleemide valdkonda, mida soovitakse lahendada[6]:

1) liikmesriikide andmekaitse regulatsioonide killustatus, õiguslik ebaselgus ja ebaühtlane rakendamine põhjustavad takistusi ettevõtete tegutsemisele ja suurendavad avaliku sektori administratiivset koormust;
2) füüsilistel isikutel on keeruline oma isikuandmete töötlemist kontrollida;
3) puudused ja vastuolud isikuandmete kaitses seoses õiguskaitseasutuste koostöö käigus toimuva andmete töötlemisega.

Eelnõus reguleeritavad küsimused on jaotatud kuude peatükki:

1) üldsätted;
2) Isikuandmete töötlemise erialused
3) Muud juhud isikuandmete töötlemisel
4) isikuandmete töötlemine õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel ja karistuste täideviimisel;
5) riiklik ja haldusjärelevalve;
6) vastutus;
7) rakendussätted.

[6] Komisjoni ettepanek andmekaitsereformi läbiviimiseks ja teised väljatöötamisega seotud dokumendid, sh komisjoni mõjuanalüüs, on kättesaadavad: http://ec.europa.eu/justice/data-protection/reform/index_en.htm (20.10.2017).

Lisaks on kõnealuse eelnõu eesmärk Eesti õigusesse üle võtta õiguskaitseasutuste direktiiv. Kuni õiguskaitseasutuste direktiivini ei olnud EL-i õiguses kehtestatud andmekaitsereegleid, mis kohalduksid politsei ja teiste pädevate asutuste tegevusele väljaspool piiriülest koostööd. Selle valdkonna reguleerimine on seni olnud liikmesriikide pädevuses. Eestis on siiani kõnealust valdkonda reguleeritud IKS-iga ning menetlusseadustikes sätestatud eranditega. Õiguskaitsevaldkonna direktiivi eesmärk on kehtestada EL-is ühtsed andmekaitsereeglid ka õiguskaitsevaldkonnas ning erinevalt raamotsusest 2008/977/JSK on direktiivi kohaldamisala laiem, hõlmates kogu andmetöötlust pädevate asutuste poolt juhul, kui selline andmetöötlus leiab aset asutuste põhiülesannete täitmise raames. Tagamaks füüsiliste isikute isikuandmete järjekindel kõrgetasemeline kaitse ka õiguskaitsevaldkonnas, sätestatakse kõnealuse eelnõuga isikuandmete töötlemise õiguslikud alused.

Eelnõu koostamisel on lähtutud arusaamast, et isikuandmete kaitse seaduse ja isikuandmete kaitse üldmääruse reguleerimisalast jääb välja isikuandmete töötlemine järgmistes õigusvaldkondades:

1. põhiseaduslike institutsioonide olemuslike ülesannete täitmine. Põhiseaduslike institutsioonidena käsitatakse Riigikogu, Riigikontrolli, õiguskantslerit ja Vabariigi Presidenti. Isikuandmete kaitse üldmäärus võib laieneda isikuandmete töötlemisele põhiseaduslike institutsioonide kantseleiliste, personali- ja varahalduse ülesannete täitmisel;
2. julgeolekuasutuste tegevus riigi julgeoleku tagamisel, mis seisneb eelkõige teabehanke raames isikuandmete töötlemises. Isikuandmete kaitse üldmäärus võib laieneda julgeolekuasutuste tegevusele kantseleiliste, personali- ja varahalduse ülesannete täitmisel ning riikliku järelevalve meetmete kohaldamisele;
3. Kaitseväe ja Kaitseliidu tegevus riigi sõjalisel kaitsmisel ja selle ettevalmistamisel ning Kaitseministeeriumi ja Riigikantselei tegevus riigi sõjalise kaitse planeerimisel. Isikuandmete kaitse üldmäärus võib laieneda isikuandmete töötlemisele Kaitseministeeriumi, Riigikantselei, Kaitseväe ja Kaitseliidu kantseleiliste, personali- ja varahalduse ülesannete täitmisel, kui need ei ole lahutamatult seotud riigi sõjalise kaitse ja selleks ettevalmistumisega.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb seitsmest peatükist:
1. Üldsätted – määratletakse seaduse reguleerimis- ja kohaldamisala.
2. Isikuandmete töötlemise erialused – sätestatakse reeglid isikuandmete töötlemiseks erijuhtudel, nagu ajakirjanduslikul, kunstilisel, akadeemilisel jne eesmärgil.
3. Muud juhud isikuandmete töötlemisel – sätestatakse reeglid erijuhtudel isikuandmete töötlemiseks.
4. Isikuandmete töötlemine õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel või karistuste täideviimisel – sätestatakse peatüki kohaldamisala, mõisted (eriliiki isikuandmed, õiguskaitseasutus), isikuandmete töötlemise põhimõtted, andmesubjekti õigused, vastutava ja volitatud töötleja kohustused, andmekaitsespetsialisti määramise kohustus ja tema ülesanded, isikuandmete töötlemise turvameetmed ja isikuandmetega seotud rikkumisest teavitamine, isikuandmete edastamine kolmandatele riikidele ja rahvusvahelistele organisatsioonidele.
5. Järelevalve – sätestatakse Andmekaitse Inspektsiooni ülesanded, pädevus, järelevalve teostamise kord ja nõuded järelevalveasutuse juhile.
6. Vastutus – nähakse ette vastutus isikuandmete töötlemise nõuete rikkumise eest.

7. Rakendussätted – nähakse ette senise IKS kehtetuks tunnistamine ja seaduse jõustumine. Samuti lisatakse rakendussäte delikaatsete isikuandmete töötlejate registri andmete kohta. Teiste seaduste muutmise sätted esitatakse eraldi eelnõuna isikuandmete kaitse seaduse rakendamise seaduse eelnõus.

Eelnõu struktuur:

1. Eelnõus kavandatu kohaselt ei reguleerita küsimusi, mis üldmäärusele tuginedes on otsekohalduva iseloomuga. Euroopa Liidu õiguse kohaselt on keelatud otsekohalduva õigusakti sisu ümber kirjutada riigi õigusesse.
2. Eelnõu liigub oma struktuurilt üldisemalt üksikule ehk kavandatu kohaselt kehtestatakse üldised alused isikuandmete kaitse seaduse kohaldamiseks ning liigutakse edasi eri iseloomuga töötlemistoimingute juurde.
3. Kuna eelnõuga võetakse üle ka õiguskaitseasutuste direktiiv, siis on eelnõus ka peatükk, mis puudutab nimetatud direktiivi ülevõtmisega seotud sätteid ehk direktiivi peatükk.
4. Direktiivi peatükile järgnevad järelevalve ja vastutuse peatükk.

Eelnõus kavandatu kohaselt reguleeritakse küsimusi, milles üldmäärus on liikmesriigile selle õiguse andnud ehk milline on diskretsiooni ulatus – kehtiva regulatsiooni säilitamine või kehtestamine/sätestamine, täpsustamine või piiramine. Eelnõu loob üldised raamid isikuandmete töötlemisele, kuid eeldab isikuandmete töötlemisega seonduvate reeglite täpsemat kehtestamist valdkonnaspetsiifilistes õigusaktides. Valdkonnaspetsiifiliste õigusaktide muudatusi käsitletakse eraldi isikuandmete kaitse seaduse rakendamise seaduse eelnõus.

§ 1. Seaduse reguleerimisala

IKS-i eelnõul on kaks suuremat eesmärki. Esimene on isikuandmete kaitse üldmääruse rakendamine ulatuses, mis liikmesriigile on antud diskretsiooniõigusega üldmääruse normide täpsustamiseks. Teine eesmärk on üle võtta direktiiv, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel või karistuste täideviimisel. Esimesel juhul tuleb sätteid lugeda koosmõjus isikuandmete kaitse üldmäärusega. Teisel juhul rakendatakse ainult Eesti õigusesse üle võetud direktiivi.

§ 2. Seaduse ja Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 kohaldamisala erisused

Kõnesoleva seaduse ning isikuandmete kaitse üldmääruse kohaldamine on seotud Euroopa Liidu aluslepingutega. Euroopa Liidu lepingu ja EL-i toimimise lepingu art 4 lõike 2 ning art 5 lõike 2 koosmõjust tuleneb, et liit austab liikmesriikide võrdsust ning nende rahvuslikku identiteeti, mis on omane nende poliitilistele ja põhiseaduslikele põhistruktuuridele, sealhulgas piirkondlikule ja kohalikule omavalitsusele. Liit austab riigi põhifunktsioone, sealhulgas riigi territoriaalse terviklikkuse tagamist, avaliku korra säilitamist ja riigi julgeoleku kaitsmist. Eelkõige riigi julgeolek jääb iga liikmesriigi ainuvastutusse. Pädevus, mida aluslepingutega ei ole liidule antud, kuulub liikmesriikidele. Samas on art 16 kohaselt igaühel õigus oma isikuandmete kaitsele ning Euroopa Parlament ja nõukogu kehtestavad seadusandliku tavamenetluse kohaselt eeskirjad füüsiliste isikute kaitse kohta liikmesriikides

liidu õiguse reguleerimisalasse kuuluva tegevuse puhul, samuti selliste andmete vaba liikumise eeskirjad.

Isikuandmete kaitse üldmääruse art 2 lõige 2 punkt a ning õiguskaitseasutuse direktiivi art 2 lõige 3 punkt a sätestavad, et uusi andmekaitse reegleid ei kohaldata sellise tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse. Koosmõjus ülaltoodud aluslepingute sättega ei reguleerita kõnesolevas seaduses seega riigikaitse ja selle ettevalmistamise ning julgeolekuasutuste tegevusega seonduvaid andmekaitse küsimusi. Vastavates valdkondades tuleb seega välja töötada erisätted, mis võimaldavad kaitsta füüsilise isiku eraelu tulenevalt põhiseaduse §-st 26. Üldmäärus kohaldub vastavaid valdkondi toetavatele funktsioonidele, nagu on kantselei töö, varahaldus vms. Erisätted tuleb kehtestada näiteks julgeolekuasutuste seadusesse, kaitseväe korralduse seadusesse ja kaitseväeteenistuse seadusesse.

Kehtivas IKS-s olid vastavad valdkonnad samuti seaduse kohaldamisalast välistatud, sest need olid kaetud riigisaladuse ja salastatud välisteabele ette nähtud erandiga. Kehtiva IKS-i § 2 lõike 3 mõte oli, et nimetatud seadust kohaldatakse riigisaladusele ja salastatud välisteabe valdkonnale niivõrd, kuivõrd see tuleneb Schengeni või Europoli konventsioonist. Viide Europoli konventsioonile ei ole enam asjakohane, sest Europoli konventsioon asendati 2009.a vastuvõetud nõukogu otsusega nr 2009/371/JSK. Praeguseks on ka see nõukogu otsus kehtetu ning Europoli tegevus on reguleeritud 11.mail 2016.a vastu võetud Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK (nn Europoli määrus). Europoli määrust kohaldatakse alates 1.maist 2017. Määruse artikkel 75 sätestab üheselt, et sellega asendatakse ja tunnistatakse kehtetuks otsus 2009/371/JSK. Seega viite lisamine Europoli konventsioonile ei ole asjakohane.

Samuti ei ole asjakohane üldseaduses viidata, et uus IKS kohaldub Europoli määrusest tulenevale andmetöötlusele, sest üldmääruse ja õiguskaitseasutuste direktiivi kohaldamisala on lai ning hõlmab kogu andmetöötlust, välja arvatud üldmääruses ja direktiivis sätestatud erandid. Europoli määrus on osa EL õigusraamistikust ning andmetöötlus leiab aset eeskätt politseitöö kontekstis, kus toimub muuhulgas andmevahetus Europoli ja riigisiseste õiguskaitseasutuste vahel. Sellisel juhul kohaldub IKS üldreegli alusel, sest andmetöötlus riigisiseste õiguskaitseasutuste poolt on hõlmatud IKS-iga (eeskätt IKS-i 4.peatükk). AKI kui järelevalveasutuse pädevus hõlmab ka järelevalve teostamist õiguskatiseasutuste poolt läbiviidavale andmetöötlusele. Sellest tulenevalt puudub vajadus säilitada uues IKS-is vana IKS-i § 2 lg 3 punktis b olevat viidet.

Erinevalt Europoli konventsioonist on Schengeni konventsioon jätkuvalt kehtiv, kuid moodustab osa EL õigusest ning seega on samuti hõlmatud nii üldmääruse kui õiguskaitseasutuste direktiivi kohaldamisalaga ja sellest tulenevalt ka uue IKS-i kohaldamisalaga. AKI pädevus teostada järelevalve Schengeni konventsiooni alusel toimuva andmetöötluse üle on samuti üheselt tuletatav tulenevalt sellest, et puudub erand, mis sellist järelevalvet välistaks ja AKI pädevus hõlmab järelevalve teostamist kogu andmetöötluse üle, millele kohaldub uus IKS (IKS § 55 lg 1). Uus IKS kohaldub isikuandmete töötlemisele õiguskaitseasutuste poolt (sh IKS 4.peatükk). Juhul, kui andmete töötlemine toimub väljaspool õiguskaitseasutuste tegevust, näiteks kui andmeid töötleb piirivalve või migratsiooniga seotud ülesandeid täitev Politsei – ja Piirivalveameti üksus, on selline andmetöötlus hõlmatud üldmääruse kohaldamisalaga ja seega laieneb sellele samuti AKI

järelevalvepädevus. Sellest tulenevalt puudub vajadus säilitada vana IKS-i § 2 lg 3 punktis a sisalduvat viidet andmetöötlusele Schengeni konventsiooni alusel.

Käesolevat seadust ja isikuandmete kaitse üldmäärust kohaldatakse süüteomenetlusele ja kohtumenetlusele menetlusseadustikes sätestatud erisustega. Vastav säte on vajalik, et täpsustada, kuidas rakendada isikuandmete kaitse õigust süüteomenetluses ja kohtumenetlustes.

Isikuandmete kaitse üldmääruse põhjenduspunkt 20 sätestab, et kui nimetatud määrust kohaldatakse muu hulgas kohtute ja muude õigusasutuste tegevuse suhtes, võiks liidu või liikmesriigi õiguses täpsustada isikuandmete töötlemise toimingud ja -menetlused, mis on seotud isikuandmete töötlemisega kohtute ja muude õigusasutuste poolt. Kohtusüsteemi sõltumatuse kaitsmiseks kohtumenetlusega seotud ülesannete täitmisel, sealhulgas otsusetegemisel, ei peaks järelevalveasutuste pädevus hõlmama isikuandmete töötlemist juhul, kui kohtud täidavad oma õigust mõistvat funktsiooni. Selliste andmetöötlustoimingute järelevalve peaks olema võimalik teha ülesandeks liikmesriigi kohtusüsteemi konkreetsetele asutustele, kes peaksid eelkõige tagama käesoleva määruse eeskirjade järgimise, teavitama kohtunikke nende käesoleva määruse kohastest kohustustest ning käsitlema selliste andmetöötlusega seotud toimingute suhtes esitatud kaebusi.

Seega on käesoleva seaduse ning isikuandmete kaitse üldmääruse kohaldamisalast väljas kohtute õigusemõistmise funktsioon. Üldmäärus kohaldub õigusemõistmist toetavatele funktsioonidele, nagu on kantselei töö, varahaldus vms.

Seoses kohaldamisalaga tuleb selgitada mõningaid probleeme, mida ei ole kõnealuses sättes otsesõnu mainitud, kuid mis on olulised uue IKS-i rakendamise seisukohast. Üldmäärus seab mitmed õigused/kohustused/põhimõtted sõltuvusse sellest, kas täidetakse avalik-õiguslikku või eraõiguslikku ülesannet. Nii näiteks sätestab üldmääruse art 6 lg 1 p e, et isikuandmete töötlemine on seaduslik, kui see on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Üldmääruse põhjenduspunkt 45 ütleb, et kui isikuandmeid töödeldakse vastavalt vastutava töötleja juriidilisele kohustusele või kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks, peaks töötlemise alus olema sätestatud liidu või liikmesriigi õigusaktis.

Määruses ei nõuta iga üksiku isikuandmete töötlemise toimingu reguleerimiseks eraldi õigusakti. Piisata võib õigusaktist, mille alusel tehakse mitu isikuandmete töötlemise toimingut vastavalt vastutava töötleja juriidilisele kohustusele või kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks. Samuti peaks töötlemise eesmärk olema kindlaks määratud liidu või liikmesriigi õigusaktis. Lisaks võiks nimetatud õigusaktis olla sätestatud kõnesoleva määruse üldtingimused, millega reguleeritakse isikuandmete töötlemise seaduslikkust, kehtestatakse tingimused vastutava töötleja kindlaksmääramiseks, töötlemisele kuuluvate isikuandmete liik, asjaomased andmesubjektid, üksused, kellele võib andmeid avaldada, eesmärgi piirangud, säilitamise aeg ja muud meetmed seadusliku ja õiglase töötlemise tagamiseks.

Põhiseaduse (PS) § 26 teine lause sätestab eraelu piiriklausli. Teise lause kohaselt võib sekkuda perekonna- ja eraellu tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Paragrahvi 26 teises lauses on seega sätestatud kvalifitseeritud seadusereservatsioon, mis lubab eraelu riivata üksnes seadusega või seaduse alusel ja § 26 teises lauses kindlaks määratud põhjustel. PS

koosmõjus isikuandmete kaitse üldmääruse art 6 lõike 1 punktiga e kannab mõtet, et isikuandmete töötlemine on võimalik seadusega või seadusel alusel antud õigusaktiga, kui see on vajalik avalikes huvides oleva ülesande või avaliku võimu teostamiseks.

Avalikes huvides oleva ülesande täitmine ei eelda, et tegu peaks olema avalikes huvides loodud institutsiooniga – haldusorgani, kohtu või põhiseadusliku institutsiooniga. Avalikes huvides olevaid ülesandeid võivad täita ka eraõiguslikud isikud. Õigusaktist võib tuleneda kohustus, et nimetatud isikud töötlevad isikuandmeid avalikes huvides oleva ülesande täitmiseks, kuid ei teosta samaaegselt avalikku võimu. Näiteks võib avalikes huvides olev ülesanne seonduda krediidiasutuste poolt teabe edastamisega avalikule võimule rahapesu ja terrorismi rahastamise tõkestamiseks. Lisaks on eriseadusi, nt avaliku teabe seadus (AvTS), mis panevad avaliku võimu teostamisele omased kohustused eraõiguslikule isikule, hõlmates teatud eraõiguslikud isikud teabevaldaja mõiste alla. „Teabevaldaja“ kasutamine ei tähenda, et eraõiguslikud isikud teostaksid avaliku võimu, vaid pigem seda, et nad täidavad avalikes huvides olevat ülesannet ja peavad avalikkusele andma neile huvipakkuvat informatsiooni. Sealhulgas võidakse ka avaldada isikuandmeid, kuid tulenevalt AvTS-st on isikuandmete avalikustamiseks seaduslik alus.

Üldmääruse põhjenduspunkt 45 lisab, et see, kas avaliku huvi või avaliku võimu teostamisega seotud ülesannet täitev vastutav töötleja peaks olema avaliku sektori asutus või muu avalik-õiguslik või eraõiguslik füüsiline või juriidiline isik, näiteks kutseliit, tuleks samuti kindlaks määrata liidu õiguses või kui see on avalikust huvist lähtuvalt põhjendatud, sealhulgas tervishoiuga seotud eesmärkidel, nagu rahvatervis ja sotsiaalkaitse ning tervishoiuteenuste juhtimine, siis liikmesriigi õiguses. Avaliku võimu teostamisele on võimalik läheneda institutsionaalselt. Haldusmenetluse seadus (HMS) sätestab §-s 8 haldusorgani mõiste, kes on seadusega, selle alusel antud määrusega või halduslepinguga avaliku halduse ülesandeid täitma volitatud asutus, kogu või isik. Lisaks haldusorganitele teostavad kõnesoleva seaduse mõttes avalikku võimu ning on seega ka osaliselt isikuandmete kaitse üldmääruse ning seaduse kohaldamisalas kohtud ja põhiseaduslikud institutsioonid.

Üldmääruse art 6 lõike 1 punkt e ja avalikule sektorile määrusega kehtestatud kohustused ei ole üks ühele samastatavad. Näiteks näeb isikuandmete kaitse üldmääruse art 37 lõike 1 punkt a ette, et avaliku sektori asutus või organ määrab andmekaitseametniku. Avaliku sektori asutused Eesti õiguse mõttes on haldusorganid ning osaliselt kohtud ja põhiseaduslikud institutsioonid. Muud isikud, kes täidavad avalikes huvides olevaid ülesandeid, peavad toodud näite puhul siiski kaaluma, kas esinevad art 37 lõike 1 punktis b toodud tingimused.

Andmekaitse Inspektsioon on oma juhendisse „Eraõiguslike avaliku teabe valdajate juhend“[1] muu hulgas koondanud Riigikohtu praktika avaliku ülesande sisustamisel. Juhendis on välja toodud järgnevad Riigikohtu seisukohad:

- Avaliku ülesande definitsiooni seaduses ei ole, kuid kohtupraktikast ja õiguskirjandusest tuleneb: avalikud ülesanded on vahetult seadusega või seaduse alusel riigile, omavalitsusele või muule avalik-õiguslikule juriidilisele isikule pandud ülesanded, või ülesanded, mis on tõlgendamise teel vastavast õigusnormist tuletatud (3-3-4-1-10).

[1] Eraõiguslike avaliku teabe valdajate juhend. Andmekaitse Inspektsioon. Täiendatud 2017. Veebis kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/avts_juhend_eraoiguslikele.pdf.

- Avalik huvi mingi teenuse olemasolu vastu iseenesest ei muuda veel seda teenust avalikuks ülesandeks. Kui eraisik osutab teenust vabatahtlikult (nt eralasteaed), nt turul valitseva nõudluse rahuldamiseks, ei täida ta avalikku ülesannet. Avalikuks ülesandeks muutub teenus seega siis, kui seda osutatakse avalik-õigusliku isiku seadusest tuleneva kohustuse täitmiseks (3-3-1-19-14, p 12).
- Avalike ülesannete puhul reguleerib avalik õigus tihti soorituse tegemise kohustust, kuid sooritus ise võib alluda eraõiguslikule regulatsioonile. Nii on see näiteks vanglapoe pidamisel – kohustus tagada kinnipeetavale sisseostude tegemise võimalus on avalik ülesanne, samas kui vanglapoes kaupade ostmine toimub eraõigusliku müügilepingu alusel (ning seejuures ei ole vahet, kas kauplust peab vangla ise või on ta selle ülesande delegeerinud eraõiguslikule isikule (3-3-1-72-11).

§ 3. Haldusmenetluse seaduse kohaldamine

Kõnesolevas seaduses ettenähtud haldusmenetlusele kohaldatakse haldusmenetluse seaduse sätteid, arvestades kõnesoleva seaduse erisusi.

§ 4. Isikuandmete töötlemine ajakirjanduslikul eesmärgil

Nii rahvusvahelises õiguses kui ka Eesti põhiseaduse §-s 45 tunnustatakse ajakirjandusvabadust. Riigil lasub üldiselt kohustus mitte sekkuda ajakirjandusvabadusse, samas on talle pandud ülesanne tagada toimiv õigusraamistik põhivabaduse toimimiseks ning adekvaatsed õiguskaitsevahendid. Ajakirjanduse kaudu või mõnel muul viisil vaba informatsiooni edastamine on väljendusvabaduse üks alaliike, mis seisneb möödapääsmatus demokraatia idee levitamises. Ajakirjandusvabadus on piiratud teiste õigustega: eraelu kaitsega, solvamise ning laimamise keeluga, valeandmete edastamise ning rassiviha õhutamise keeluga, samuti alaealiste ohustamise jms keeluga. Ajakirjandusvabaduse olemuslikud tunnused tähendavad täiendavate garantiide loomist ajakirjanikele nende erialases tegevuses ning nende allikate saladuse kaitset. Ajakirjaniku võimalus mitte avaldada oma informatsiooniallikaid tagab talle selliste allikate paljususe ja soodustab tegelikku infovabadust. Ajakirjanikel oleks kahtlemata väga raske teha põhjalikke uurimuslugusid, kui nad peaksid hiljem osalema tunnistajatena kohtulikus uurimises. Ajakirjaniku missioon on teha avalikuks asjaolud ja sündmused, informeerides nii avalikkust talle teada olevatest olulistest juhtumitest.

Ajakirjandusvabaduse ning eraelu puutumatuse ja isikuandmete kaitse õiguse tasakaalustamiseks on isikuandmete kaitse üldmääruse artiklis 85 antud liikmesriikidele võimalus näha ette vabastusi ja erandeid üldmääruses sätestatud kohustustest. Üldmääruse põhjenduspunktis 153 on kehtestatud, et liikmesriigid peaksid sellised vabastused ja erandid vastu võtma üldpõhimõtete, andmesubjekti õiguste, vastutava töötleja ja volitatud töötleja, isikuandmete kolmandatele riikidele ja rahvusvahelistele organisatsioonidele edastamise, sõltumatute järelevalveasutuste, koostöö ja ühtsuse ning andmete töötlemise eriolukordade kohta. Kui sellised vabastused või erandid erinevad liikmesriigiti, tuleks kohaldada selle liikmesriigi õigust, mida kohaldatakse vastutava töötleja suhtes.

Selleks et võtta arvesse sõnavabadusõiguse tähtsust igas demokraatlikus ühiskonnas, tuleb laialt tõlgendada selle vabadusega seonduvaid kontseptsioone, näiteks ajakirjandust. Seetõttu on ka kõnesolevas eelnõus jäetud isikuandmete ajakirjanduslik töötlemine täpsemalt

määratlemata. Andmekaitse Inspektsioon on oma meediat käsitlevas juhendis selgitanud, keda võib isikuandmete ajakirjanduslikul eesmärgil töötlemisena silmas pidada. Meediana käsitletakse nii professionaalset meediat (päeva- ja nädalalehed, tele- ja raadiokanalid) kui ka blogisid, netifoorumeid ja suhtlusvõrgustikke. Mõlemad võivad sisaldada ajakirjandusliku eesmärgiga artikleid ning puhtalt meelelahutuslikku osa. Erinevalt meelelahutusest on ajakirjanduslikul eesmärgil lubatud isikuandmeid avalikustada ka ilma inimese enda nõusolekuta.[7]

Kõnesolevas eelnõus on säilitatud kehtiv regulatsioon, mille järgi isikuandmeid võib andmesubjekti nõusolekuta töödelda ajakirjanduslikul eesmärgil, eelkõige avalikustada meedias, kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega. Isikuandmete avalikustamine ei tohi ülemäära kahjustada andmesubjekti õigusi. Vastava sättega on ajakirjandusele antud lisaks üldmääruse artiklites 6 ja 9 sätestatud isikuandmete töötlemise alustele erialus. Erialus võimaldab teha erandi kõikides eeltoodud artiklites nimetatud töötlemise alustest. Liikmesriigile on jäetud võimalus vastavalt oma õiguskorrale, eelkõige vastavalt põhiseadusele, otsustada, kuidas tasakaalustada eraelu puutumatust ja ajakirjandusvabadust.

Üheks oluliseks suunanäitajaks ajakirjandusvabaduse ja eraelu puutumatuse huvide kaalumisel on Euroopa Inimõiguste Kohtu (EIK) otsus asjas Hannover *vs*. Saksamaa[8] (tuntud ka kui printsess Caroline'i kaasus). Monaco printsess Caroline (kes ei täida Monaco vürstiriigi ametlikke funktsioone) oli alates 1990ndatest üle kümne aasta üritanud takistada oma eraelu kajastavate fotode avaldamist Euroopa riikide kõmulehtedes. Selles kohtuasjas olid vaidlusaluseks Saksa tabloidväljaandes avaldatud pildid, mis kujutasid teda nt hobuse seljas, tegemas sisseoste üksi ja ihukaitsjaga, istumas restoranis koos Prantsuse näitlejaga, suusapuhkusel Austrias, lahkumas üksi ja koos prints Ernst August von Hannoveriga oma Prantsuse residentsist ning komistamas Monte Carlo rannaklubis takistusele. Kohus leidis, et viidatud piltide avaldamine meediaväljaandes rikub printsess Caroline'i õigusi. Oluliseks teguriks eraelu puutumatuse ja sõnavabaduse tasakaalustamisel tuleb kohtu hinnangul pidada asjaolu, kas ajakirjanduses avaldatavad faktid (sh ka fotod) aitavad kaasa diskussiooni tekkimisele demokraatlikus ühiskonnas. Sel juhul oli fotode avaldamise eesmärk vaid teatud lugejaskonna uudishimu rahuldamine ning meedia majandushuvide kindlustamine. Kohus on lahendis võtnud lähtealuseks funktsiooni, mida isik täidab, mitte selle, kas tegemist on isiku avaliku või eraeluga. Seega nt foto, millel printsess avab ostukeskust, ei riiva tema eraelu, ent foto, millel kujutatakse printsessi samas ostukeskuses tegemas järgmisel päeval sisseoste, riivab. Kui avaliku elu tegelane on avalikus kohas, kuid ei täida avaliku elu tegelase ülesandeid, on tegemist tema eraeluga.

EIK on mitmel korral väljendanud ka seisukohta[9], et poliitikud peavad taluma märksa ulatuslikumat kriitikat kui lihtsalt avaliku elu tegelased. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni (EIÕK) art 10 lõiget 2 ei kohaldata EIK hinnangul mitte

---

[7] Isikuandmete avalikustamine meedias: Andmekaitse Inspektsiooni sekkumiskriteeriumid - http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/meediavaidlusse%20sekkumise%20kriteeriumid.pdf.

[8] Euroopa Inimõiguste Kohus. Von Hannover vs. Saksamaa. Veebis kättesaadav: http://194.242.234.211/documents/10160/2055471/EHCR+ +CASE+OF+VON+HANNOVER+v.+GERMANY+No.+2.pdf.

[9] Dabrowski *vs*. Poola, EIK 19.12.2006.

ainult „informatsioonile“ ja „ideedele“, mida käsitatakse üldiselt kui kahjutuid või neutraalseid, vaid ka solvavatele, šokeerivatele või häirivatele teadetele. Sellised on pluralismi, tolerantsuse ja eelarvamustevaba suhtumise nõuded, ilma milleta ei eksisteeriks ka demokraatlikku ühiskonda[10]. Konventsiooni art 10 lõige 2 hõlmab endas ka väheses ulatuses piiranguid poliitilistele kõnedele või debatile avaliku huvi küsimustes. Veelgi enam, aktsepteeritava kriitika piirid on laiemad poliitiku kui muu eraisiku puhul. Võttes arvesse ajakirjanduse silmapaistvat rolli, peab press siiski eristama informatsiooni ja ideesid poliitilistes küsimustes ja teistes avaliku huvi asjades.

Ajakirjandusvabadus võimaldab üldsusele parima meetme arvamuse kujundamiseks oma poliitiliste liidrite ideede ja hoiakute kohta. Ajakirjandusvabadus hõlmab ka võimaluse tugineda teatud astmeni liialdustele või koguni provokatsioonidele. Poliitikud peavad üles näitama suuremat tolerantsust kriitika suhtes. Ehkki väljendusvabadus allub eranditele, peavad nad neid erandeid tõlgendama kitsendavalt ning vajadus piirangute järele peab olema veenvalt tuvastatud. Nii on EIK ka leidnud, et trükised, mis sisaldasid kahe poliitiku kriitikat poleemilises ja sarkastilises keeles, kahtlemata riivasid ja šokeerisid neid, ent olles valinud oma elukutse, asetasid poliitikud end ise tugeva kriitika ja huvi objektiks ning see on koormis, mida nad peavad taluma demokraatlikus ühiskonnas[11]. Poliitik paljastab vältimatult ja teadlikult iga oma sõna ja teo tihedale kontrollile ajakirjanduse ja avalikkuse poolt ning peab seetõttu väljendama suuremat taluvusastet. EIK on omistanud kõige kõrgemat tähtsust väljendusvabadusele poliitilise debati kontekstis ning leidnud, et väga tugevad argumendid on nõutavad, et õigustada poliitiliste kõnede piiranguid.

Seoses avaliku elu tegelaste fotode avaldamisega on Ühendkuningriigi kohus teinud otsuseid, millest on võimalik esile tuua mõningaid elemente, mida tuleks arvestada. Eraelu puutumatuse riive intensiivsuse hindamisel on kohus kaalunud kõiki ümbritsevaid asjaolusid, nt mida foto kujutab, kes on subjekt, kus ja kuidas see foto tehtud on. Eraelu puutumatuse proovikiviks on kahtlemata asjaolu, kas isikul oli mõistlik ootus eraelu puutumatusele. Nii nt leidis Ühendkuningriigi kohus asjas Campbell *vs.* MGN Ltd, et ajalehes ilmunud uudist ilmestanud foto avaldamine ei olnud põhjendatud. Tegemist oli juhtumiga, kus tuntud modelli, kes oli avalikkuses eitanud igasugust narkootiliste ainete tarbimist, fotografeeriti, kui ta väljus anonüümsete narkomaanide regulaarselt kohtumiselt ning uudis ja seda illustreerinud foto avaldati laia levikuga ajalehes. Anonüümsed alkohoolikud ja anonüümsed narkomaanid ei kasuta sellist nimetust lihtsalt efekti pärast. Nad pakuvad neile, kes otsivad abi, anonüümsust nende endi kaitseks. Kui avalikkusele tekitatakse mulje, et inimeste sellised meditsiiniandmed ja fotod, mis kujutavad neid osalemas ravikohtumistel, võivad saada avalikuks, siis mõtlevad nad suure tõenäosusega hoolikalt järele, enne kui lähevad vajalikule ravile. Ja see oleks vastuolus nii avaliku huviga kui ka ühiskonna huvidega tervikuna. [12]

EIK on leidnud, et teatud sündmustele pereelus tuleb anda eriliselt hoolikas kaitse. Lähedase surm ja sellele järgnev lein kohustavad mõnikord võimuorganeid võtma meetmeid, et austada puudutatud isikute eraelu ja perekonnaelu. Tegemist oli fotoga, mis kujutas tapetud prefekti surnukeha mõni hetk pärast mõrva ning mis avaldati kõigest 13 päeva pärast mõrva ja 10

---

[10] Hanyside *vs*. Ühendkuningriik, EIK 07.12.1976.
[11] Ukrainian Media Group *vs*. Ukraina, EIK 29.03.2005.
[12] Lordide Koja 06.05.2004 otsus asjas Campbell *vs*. MGN Ltd. Kättesaadav aadressil: http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm.

päeva pärast matuseid. Seetõttu leidis kohus, et lein, mida ohvri perekond tundis, pidanuks ajakirjanikke panema ilmutama taktitunnet ja ettevaatlikkust, kuna surma asjaolud olid vägivaldsed ja traumaatilised ohvri perekonna jaoks.[13]

Teatud isikute puhul on EIK leidnud, et eraelu puutumatuse piirid ulatuvad kaugemale. EIK on omistanud kõige kõrgemat tähtsust väljendusvabadusele poliitilise debati kontekstis ning leidnud, et poliitiliste kõnede piirangute õigustamiseks on nõutavad väga tugevad argumendid. Konventsiooni art 10 lõige 2 hõlmab endas ka väheses ulatuses piiranguid poliitilistele kõnedele või debatile avaliku huvi küsimustes. Veelgi enam, EIK hinnangul on aktsepteeritava kriitika piirid poliitiku puhul laiemad võrreldes eraisikuga. Võttes arvesse ajakirjanduse silmapaistvamat rolli, peab press siiski eristama informatsiooni ja ideesid poliitilistes küsimustes ja teistes avaliku huvi asjades. Ajakirjandusvabadus võimaldab üldsusele parima meetme oma poliitiliste liidrite ideede ja hoiakute kohta arvamuse kujundamiseks, tagades ühtlasi ka võimaluse tugineda seejuures teatud astmeni liialdustele või koguni provokatsioonidele.

Ajakirjanduslikul eesmärgil isikuandmete töötlejad on kohustatud järgima isikuandmete kaitse üldmäärusest tulenevaid nõudeid. Selleks et paremini tasakaalustada ajakirjandusvabaduse teostamist ning õigust eraelu ja isikuandmete kaitsele, on kõnesolevas eelnõus mõningad erandid, mis peaksid hõlbustama ajakirjandusvabaduse teostamist. Esmalt on analoogselt varasema regulatsiooniga säilitatud õigus töödelda isikuandmeid andmesubjekti nõusolekuta avaliku huvi korral. See tähendab, et ajakirjanduslikul eesmärgil isikuandmeid töötlev isik ei pea lähtuma tavapärastest isikuandmete töötlemise õiguslikest alustest, mis on sätestatud üldmääruse artiklis 6. Näiteks ei ole vaja küsida andmesubjekti nõusolekut. Samas on ajakirjanduslikul eesmärgil isikuandmeid töötlev isik kohustatud järgima isikuandmete kaitse põhimõtteid, sealhulgas, kas isikuandmeid töödeldakse minimaalselt vajalikul määral, et saavutada oma eesmärk. Oluline on ka andmete aja- ja asjakohasuse kontroll.

Lähtuvalt eeltoodud kohtupraktikast ning ajakirjanduse olulisest rollist ühiskonnas on isikuandmete töötlemine ajakirjanduslikul eesmärgil lubatud, kui selleks on avalik huvi. Avalik huvi kaalub üles andmesubjekti õiguste kaitse. Andmesubjekti õiguste kaitse tase on viidud allapoole ning sätestatud, et ajakirjanduslikul eesmärgil isikuandmete töötleja peab analüüsima, kas töötlemisega ei kaasne ülemäärast andmesubjekti õiguste ja vabaduste kahjustamist. Kui andmesubjekti õiguste ja vabaduste kahjustamine esineb, kuid see ei ole ülemäärane, võib isikuandmeid töödelda. Avalik huvi on tuletatud ülaltoodud kohtupraktikast ning sellest, et ajakirjanduslik isikuandmete töötlemine peab aitama kaasa diskussiooni tekkimisele demokraatlikus ühiskonnas.

Üksikisikul on ootus eraelu puutumatusele. Üksikisiku andmete kajastamine ajakirjanduse poolt peab olema põhjendatud millegi väga olulisega, et sekkumine tema eraellu oleks proportsionaalne. Seega võib ajakirjandus isikuandmeid töödelda ka sellises olukorras, kus esineb andmesubjekti õiguste või vabaduste riive. Alles siis, kui esineb ülemäärane õiguste või vabaduste riive, tuleb kaaluda, kas avalik huvi kaalub üles andmesubjekti õiguste riive.

---

[13] Hachette Filipacchi Associes *vs*. Prantsusmaa, EIK 14.06.2007.

Kõnesolevas paragrahvis toodud kriteeriume on vaja kaaluda igakordse isikuandmete töötlemise juures. Oluline on tähele panna, et ajakirjanduslikul eesmärgil töötlemise korral tuleb iga töötlemistoimingu puhul eraldi hinnata, kas selleks on õigus kasutada erandeid. Avalikustamine on üks põhilisemaid isikuandmete töötlemise toiminguid, kuid analüüsida oleks vaja ka säilitamist, otsingumootoritele kättesaadavaks tegemist, edastamist kolmandatele isikutele ning arhiveerimist või kustutamist. Muuhulgas tuleb tähele panna ka isikuandmete kaitse üldmääruse art 6 lõikes 4 sätestatud isikuandmete edasise töötlemise tingimusi.

§ 5. Isikuandmete töötlemine akadeemilise, kunstilise ja kirjandusliku eneseväljenduse tarbeks

Üldmääruse artikkel 85 võimaldab liikmesriigil kehtestada muu hulgas normid, mis käsitlevad isikuandmete töötlemist kunstilise ja kirjandusliku eneseväljenduse tarbeks. Nimetatud eesmärgil isikuandmete töötlemine võimaldab liikmesriigil kehtestada vabastusi ja erandeid üldmääruse artikli lõikes 2 sätestatust.

Regulatsioon kunstilise ja kirjandusliku eneseväljenduse tarbeks on vajalik nt raamatute, filmide, aga ka kujutava kunsti teoste jaoks (nt kui kasutatakse isiku kujutist kujutava kunstiteose loomisel), kui need ei kvalifitseeru ajakirjanduseks. Samuti tuleks arvesse võtta elulooraamatute ja -filmide populaarsuse kasvu, mille raames käsitletakse ka kogu ühiskonna jaoks väga olulisi teemasid, nagu naiste- või lastevastane vägivald, pagulasküsimused jne.

Nimetatud küsimuse reguleerimine uues seaduses ei ole oluline vaid seetõttu, et üldmäärus sellise õiguse liikmesriigile annab, vaid see vajadus on tingitud ka mitmest kohtuasjast, mille raames on vaidlustatud isikuandmete avalikustamise õiguspärasust nii kinokunstis kui ka kirjanduses. Samuti on pidanud Andmekaitse Inspektsioon selle küsimusega kokku puutuma oma nõustamispraktikas, kui on olnud vaja töödelda isikuandmeid kõnesolevas paragrahvis sätestatud eesmärkidel.

Näiteks on Riigikohus oma lahendis nr 3‑2‑1‑153‑16[14] käsitlenud küsimusi, mis puudutab isikuandmete avaldamise õiguspärasust elulooraamatus, samuti nõusoleku andmist ja selle tagasivõtmise õiguslikke tagajärgi. Kohtulahendis on analüüsitud ka ajakirjanduslikul eesmärgil töötlemise erisuse kohaldamist elulooraamatule. Samuti on Riigikohus oma lahendis nr 3-2-1-104-09[15] käsitlenud isikuandmete avalikustamist filmis ja selle õiguspärasust.

Praegu kehtivas IKS-is puudub konkreetne õiguslik alus isikuandmete töötlemiseks akadeemilise, kunstilise või kirjandusliku eneseväljenduse tarbeks. Tagamaks isikuandmete

---

[14] Riigikohtu tsiviilkolleegiumi otsus nr 3‑2‑1‑153‑16, https://www.riigikohus.ee/et/lahendid?asjaNr=3-2-1-153-16&sortVaartus=LahendiKuulutamiseAeg&sortAsc=false&kuvadaVaartus=Sisu&pageSize=25&defaultPageSize=25.

[15] Riigikohtu tsiviilkolleegiumi otsus nr 3-2-1-104-09 https://www.riigikohus.ee/et/lahendid?asjaNr=3-2-1-104-09&sortVaartus=LahendiKuulutamiseAeg&sortAsc=false&kuvadaVaartus=Sisu&pageSize=25&defaultPageSize=25.

töötlemise õiguspärasust sel eesmärgil, toimitakse praktikas põhimõtteliselt kahte moodi: andmesubjekt annab selleks nõusoleku või sõlmitakse vastavasisuline tsiviilõiguslik leping.

Kui aga analüüsida põgusalt nõusoleku kui õigusliku aluse olemust, siis nii kehtiva IKS-i järgi kui ka üldmääruses sätestatu kohaselt võib nõusoleku igal ajal tagasi võtta, mis aga selgelt võib kaasa tuua majandusliku surve nii elulooraamatute kui ka -filmide tootjatele ja tegijatele. Õigus nõusolek igal ajal tagasi võtta võib kaasa tuua ebaproportsionaalseid pingutusi filmide ja elulooraamatute tegijatele, mis võib selgelt kahjustada ka sõna- ja teabevabaduse olemust tervikuna.

Kõnesoleva paragrahviga sätestatakse õigus töödelda isikuandmeid ilma andmesubjekti nõusolekuta, kui see ei kahjusta andmesubjekti õigusi. Selle paragrahvi olemus seisneb isikuandmete kaitse kaudu tasakaalu leidmises kahe põhiõiguse vahel – sõna- ja teabevabadus ning õigus eraelu kaitsele. Seega eeldab isikuandmete töötlemine ilma andmesubjekti nõusolekuta kõnesolevas paragrahvis sätestatud eesmärgil ikkagi iga kord, et tuleb kaaluda võimalikke ohte, mis võivad tekkida andmesubjekti õigustele. Võrreldes isikuandmete töötlemisega ajakirjanduslikul eesmärgil, on käesolevas sättes andmesubjekti õiguste ja vabaduste kaitse tase kõrgem. Hinnata tuleb andmesubjekti õiguste ja vabaduste kahjustamist, mitte ülemäärast kahjustamist.

§ 6. Isikuandmete töötlemine teadus-, ajaloouuringu ja riikliku statistika vajadusteks

Üldmääruse art 89 võimaldab liikmesriikidel sätestada teadus-, ajaloouuringute ja statistilisel eesmärkidel töötlemisele erandeid andmesubjektidele sätestatud õigustest. Praegu kehtiva IKS paragrahv 16 reguleerib samuti isikuandmete töötlemist teadus-, ajaloouuringu või riikliku statistika vajadusteks. Eelnõuga plaanitakse säilitada kehtiv regulatsioon, kuid täiendades seda eranditega, mis tulenevad üldmääruse art 89, ning kehtestatakse ka kaitsemeetmed, mis peavad olema tagatud vastavalt üldmääruse art 89, kui isikuandmeid töödeldakse kõnesolevas paragrahvis sätestatud eesmärkidel. Säte põhineb ka üldmääruse art 6 lõike 1 punktil e, kus liikmesriigil on võimalik õigusaktiga täpsustada avalikes huvides oleva ülesande täitmise aluseid. Teadus- ja ajaloouuringud ning riiklik statistika on avalikes huvides olevad ülesanded.

Üldmääruse põhjenduspunkti 159 kohaselt tuleks teadusuuringute eesmärgil toimuvat isikuandmete töötlemist tõlgendada nii laialt, et see hõlmab näiteks:

1) tehnoloogiaarendust ja tutvustamistegevust;
2) alusuuringuid, rakendusuuringuid ja erasektori vahenditest rahastatavaid uuringuid, lisaks tuleks arvesse võtta EL-i toimimise lepingu artikli 179 lõikes 1 sätestatud liidu eesmärki luua Euroopa teadusruum;
3) rahvatervise valdkonnas avalikust huvist lähtuvad uuringud.

Teadus- või ajaloouuringute eesmärgil isikuandmete töötlemise eripära arvessevõtmiseks tuleks kohaldada eritingimusi eelkõige seoses isikuandmete avaldamise või muul viisil avalikustamisega teadusuuringute eesmärgi kontekstis. Kui teadusuuringute tulemus eelkõige tervishoiu kontekstis loob aluse täiendavateks meetmeteks andmesubjekti huvides, tuleks nende meetmete suhtes kohaldada käesoleva määruse üldiseid eeskirju.

Statistiline eesmärk tähendab kõiki isikuandmete kogumise ja töötlemise toiminguid, mis on vajalikud statistikauuringuteks või statistika koostamiseks. Koostatud statistikat võib edasi

kasutada muul eesmärgil, ka teadusuuringute eesmärgil. Statistiline eesmärk eeldab, et töötlemise tulemus ei ole isikuandmed, vaid koondandmed, ning et seda tulemust või isikuandmeid ei kasutata ühtegi konkreetset füüsilist isikut puudutavate meetmete või otsuste toetamiseks.

Eelnõu paragrahvi 6 lõike 1 kohaselt võib andmesubjekti nõusolekuta teadusuuringu või riikliku statistika vajadusteks isikuandmeid töödelda eelkõige pseudonüümitud või samaväärset andmekaitse taset võimaldaval kujul. Pseudonüümimise all tuleb mõista üldmääruse art 4 punktis 4 sätestatut.

Seoses tehnoloogilise kiire arenguga, sealhulgas privaatsust toetavate tehnoloogiate arenguga[16], on põhjendamatu piirata andmesubjekti nõusolekuta töötlemist pseudonüümimisega, eesmärk peab olema ennekõike see, et tagatud on andmesubjektide põhiõigused ja -vabadused. Näiteks võivad olla samaväärsed tehnoloogiad kodeerimine või muu selline viis, mis eraldab isikuandmed teistest andmetest ja võimaldab viimaseid töödelda analüüside koostamiseks. Oluline on ka märkida, et isikustamata kujul olevatele andmetele ei kohaldata isikuandmete kaitse üldmäärust. See tähendab, et isikustamata, näiteks anonüümitud andmetele ei ole vaja kohaldata kõnesoleva eelnõu teadusuuringute ja statistika kohta käivat sätet. Anonüümse andmeanalüüsi korral ei tule järgida isikuandmete kaitse õiguse reegleid. Kui analüüse koostatakse pseudonüümitud või mõnel muul viisil andmesubjekti mittetuvastataval kujul, siis tuleb järgida isikuandmete kaitse üldmääruse norme, kuid selleks ei ole vaja küsida eelnevalt Andmekaitse inspektsiooni luba.

Teatud teadusuuringute puhul on vajalik eelnev Andmekaitse Inspektsiooni või eetikakomitee luba. Luba on vajalik, kui uuring tehakse andmesubjekti tuvastada võivate andmetega ning kasutatakse isikuandmete eriliike. Loa uuringu teostamiseks annab vastava valdkonna eetikakomitee. Kui eetikakomiteed ei ole loodud, siis annab loa uuringu tegemiseks Andmekaitse Inspektsioon. Välja tuleb tuua, et eetikakomitee või Andmekaitse Inspektsiooni luba ei ole vaja, kui esmalt andmed pseudonüümitakse või anonüümitakse. See tähenda, et isikut mittetuvastavale kujule viimine ei vaja eraldi luba. Luba on vaja siis, kui kogu analüüs põhineb jooksvalt andmesubjekti tuvastada lubavatel isikuandmete eriliikidel. Oluline on ka märkida, et eelnev loakohustus ei hõlma ajaloouuringuid või riikliku statistika vajadusteks koostatavaid analüüse.

Eelnõusse on lisatud ka säte, mille kohaselt loetakse käesoleva seaduse tähenduses teadusuuringuks täidesaatva riigivõimu poliitika kujundamise eesmärgil tehtud uuringud. Kui nimetatud eesmärgil tehakse päringuid teise vastutava või volitatud töötleja andmekogusse või kasutatakse teise vastutava või volitatud töötleja vastutusalas olevaid andmete kogumeid, siis tuleb küsida Andmekaitse Inspektsiooni luba. Teise vastutava või volitatud töötleja andmekoguna peetakse silmas olukorda, kus näiteks üks ministeerium soovib teise ministeeriumi käest saada andmeid, et koostada taustamaterjali mõne eelnõu koostamiseks. Samuti on see oluline, et koostada näiteks eelnõu seletuskirjades olevaid mõjuanalüüse.

Näite poliitika kujundamise eesmärgil tehtavast teadusuuringust võib tuua sisserände piirarvu töörühma tööst. Vaja oli analüüsida, kui palju on viimase paari aasta jooksul nii sisserändajad

[16] 2017 Privacy Tech Report. Veebis kättesaadav: https://iapp.org/resources/article/2017-privacy-tech-vendor-report/.

üldse kui ka sisserände piirarvu alusel tööle tulnud inimesed riigile tulu- ja sotsiaalmaksu maksnud, näitamaks nende rolli Eesti majanduses ja tööjõuturul. Vastavas uuringus pidid andmeid vahetama kaks valitsusasutust, sest teave töö- ja elamislubade ning laekunud maksude kohta asub eri andmekogudes. Kuigi uuringu tulemused on anonüümitud kujul ja üldistatud, tuleb selle läbiviimiseks kasutada isikustatud kujul andmeid.

§ 7. Isikuandmete töötlemine avalikes huvides toimuva arhiveerimise eesmärgil

Üldmääruse art 89 võimaldab liikmesriikidel sätestada avalikes huvides toimuva arhiveerimise eesmärgil erandeid andmesubjektidele sätestatud õigustest. Tegemist on küsimusega, mida ei ole reguleeritud praegu kehtivas IKS-is.

Eelnõus on kirjas, et kui isikuandmeid töödeldakse avalikes huvides toimuva arhiveerimise eesmärgil, võib vastutav või volitatud töötleja Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklites 15, 16, 18, 20 ja 21 sätestatud andmesubjekti õigusi piirata niivõrd, kuivõrd nende õiguste teostamine tõenäoliselt muudab võimatuks avalikes huvides toimuva arhiveerimise eesmärgi saavutamise või takistab seda oluliselt. Nimetatud andmesubjekti õigusi võib piirata selleks, et mitte ohustada arhiivis sisalduvate dokumentide seisundit, nende autentsust, usaldusväärsust, terviklikkust ja kasutatavust. Viimasesse lausesse on lisatud eesmärk, miks võib andmesubjekti õigusi piirata. Kui andmesubjekti õiguste või vabaduste piiramine on mingil põhjusel vajalik, kaalutakse piirangute vajalikkust arhiivis olevate dokumentide seisundi, autentsuse, usaldusväärsuse ja kasutatavusega.

Eelnõus kehtestatavad erandid andmesubjekti õiguste ja vabaduste piiramiseks on proportsionaalsed ja vajalikud arhiveerimise eesmärgi täitmiseks. Arhivaalide originaalides parandusi ei tehta, sest üks arhiivi- ja dokumendihalduse põhiprintsiip on hoida dokumente autentsetena. Asutus hoiab ning kasutab dokumente selliselt, et see ei kahjusta nende seisundit ega ohusta nende autentsust, usaldusväärsust, terviklikkust ja kasutatavust (Arhiivieeskiri § 3 lg 4). Ebaõigete andmete parandamist ja mittetäielike isikuandmete täiendamist võib andmesubjekt taotleda ja seda saab teha arhivaali kirjeldavates andmetes. See ei pea tingimata toimuma üldmääruse kohases vastuväidete esitamise vormis. Vajadusel lisatakse arhivaalile õiend ebakorrektsete andmete kohta.

Arhivaalide töötlemist reguleerib täpsemalt arhiiviseadus (ArhS) ja selle alusel antud määrus, mis on eriõigusakt kõnesoleva seaduse ja isikuandmete kaitse üldmääruse suhtes. Andmesubjekt ei esita arhiivile klassikalisel kujul taotlusi oma andmetega tutvumiseks, vaid selleks on loodud elektrooniline lahendus. Andmesubjekt saab vajaduse korral ise arhivaalidest otsida, kas tema isikuandmeid on kunagi töödeldud. Kui vaja, saab arhiiv teda juhendada. Igakordne andmesubjektile vastamine tema andmete töötlemise kohta tekitab arhiivi seisukohast ebamõistlikku halduskoormust. Riigilõivuseadusest tulenevad tasumäärad arhiiviteatise väljastamise eest. Lisaks reguleerib tasusid ArhS § 3 lõike 4 alusel antud tasuliste teenuste loetelu ja tasu määrade määrus.

§ 8. Lapse isikuandmete töötlemine infoühiskonna teenuste pakkumisel

Eelnõu § 8 reguleerib küsimust, kui infoühiskonna teenuseid pakutakse lastele, ning määrab vanuse, millal lapse antud nõusolek on õiguspärane. Tegemist on uue küsimusega, mida ei ole reguleeritud kehtivas IKS-is. Üldmääruse art 8 lõike 1 kohaselt võivad liikmesriigid sätestada

madalama vanuse, tingimusel et madalam vanus ei ole alla 13 aasta. Üldmääruse art 8 lõike 3 kohaselt ei mõjuta üldmääruse art 8 lõige 1 liikmesriikide üldist lepinguõigust.

Üldmääruse põhjenduspunkti 38 kohaselt väärivad laste isikuandmed erilist kaitset, kuna lapsed ei pruugi olla piisavalt teadlikud asjaomastest ohtudest, tagajärgedest ja kaitsemeetmetest ning oma õigustest seoses isikuandmete töötlemisega. Niisugune eriline kaitse peaks eelkõige rakenduma laste isikuandmete kasutamisel turunduse eesmärgil või isiku või kasutajaprofiili loomiseks ja laste isikuandmete kogumisel otse lastele pakutavate teenuste kasutamise puhul. Vanemliku vastutuse kandja nõusolekut ei peaks olema vaja seoses lapsele otse pakutavate ennetavate või nõustamisteenustega.

Üldmääruse põhjenduspunkti 58 järgi peaks laste isikuandmete töötlemisel kogu teave olema selges ja lihtsas keeles, mis on lapsele kergesti arusaadav, samamoodi tuleb ka lapsega suhelda.

Eelnõus kavandatu kohaselt on lapse isikuandmete töötlemine infoühiskonna teenuste pakkumisel seaduslik üksnes juhul, kui laps on vähemalt 13-aastane. 13 aasta piir on kehtestatud eri osapoolte ettepanekul ning toodud kooskõlastusringi käigus aasta võrra madalamale.

§ 9. Isikuandmete töötlemine pärast andmesubjekti surma

Eelnõu paragrahvis 9 reguleeritakse isikuandmete töötlemist pärast andmesubjekti surma. Tegemist on küsimusega, mis jääb üldmääruse kohaldamisalast välja, kuid selle põhjenduspunkt 27 näeb liikmesriikidele ette võimaluse seda küsimust oma riigi õiguses reguleerida.

Isikuandmete töötlemine pärast andmesubjekti surma on ka reguleeritud kehtiva IKS-i paragrahvis 13.

Andmesubjekti nõusolek kehtib andmesubjekti eluajal ja 30 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. Andmesubjekti nõusolek eriliiki isikuandmete töötlemiseks kehtib 80 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. Uuena on eelnõusse lisatud eriliiki isikuandmete töötlemise piirangud. Piirang nende andmete töötlemiseks kehtib 80 aastat tärast andmesubjekti surma. Vastava piirangu eesmärk on kaitsta andmesubjekti lähedasi. Näiteks piirata surnud lapse terviseandmete töötlemist pikemat aega pärast tema surma, et kaitsta tema vanemate eraelu.

Pärast andmesubjekti surma on tema isikuandmete töötlemine lubatud andmesubjekti pärija nõusolekul, välja arvatud juhul, kui isikuandmete töötlemiseks ei ole nõusolekut vaja. Vastav alus viitab kõnesoleva paragrahvi viimasele lõikele, kus andmesubjekti nime, sugu, sünni- ja surmaaega ning surma fakti on lubatud töödelda andmesubjekti nõusolekuta. Teisel alusel on andmeid lubatud töödelda, kui andmesubjekti surmast on möödunud 30 aastat või isikuandmete eriliikide töötlemise korral 80 aastat. Viimane alus viitab muudele õiguslikele alustele. Isikuandmete kaitse üldmääruses on nii artiklites 6 ja 9 kui ka erandlikel juhtudel (ajakirjandus, kunstiline eneseväljendus, arhiivid jne) sätestatud erinevad isikuandmete töötlemise õiguslikud alused. Vastava aluse olemasolul võib samuti isikuandmeid töödelda. Ainult nõusolekule viitamine kitsendaks põhjendamatult isikuandmete töötlemise aluseid.

Pärijana käsitatakse kõnesolevas eelnõus pärijat pärimisseaduse (PärS) § 4 lõike 1 ja § 130 lõike 1 tähenduses. Pärandi avanemisel läheb pärand üle pärijale. Pärandi vastuvõtmisega lähevad pärijale üle kõik pärandaja õigused ja kohustused, välja arvatud need, mis oma olemuselt on lahutamatult seotud pärandaja isikuga või mis seadusest tulenevalt ei saa ühelt isikult teisele üle minna. Pärijal on võimalik pärandaja nõusolekut muuta osas, mis ei ole eeltoodust tulenevalt lahutamatult seotud pärandaja isikuga.

Mitme pärija olemasolul on andmesubjekti isikuandmete töötlemine lubatud neist ükskõik kelle nõusolekul.

§ 10. Isikuandmete töötlemine seoses võlakohustuse rikkumisega

Eelnõu § 10 sätestab isikuandmete töötlemise üldreeglid krediidivaldkonnas. Nimetatud küsimus on reguleeritud ka praegu kehtivas IKS-is.

Reguleerimise vajadus tuleneb soovist tagada võimalus isikute finantsilise usaldusväärsuse ehk krediidivõimelisuse hindamiseks. On olemas praktiline vajadus selleks, et finantsasutused ning äriettevõtted saaksid hinnata teise lepingupoole usaldusväärsust lepinguliste suhete täitmisel. Üks kriteerium isiku usaldusväärsuse hindamisel on see, kuidas isik on käitunud oma seniste lepinguliste kohustuste täitmisel. Oluline on, et töödelda võib vaid lepinguliste kohustuste rikkumist käsitlevaid andmeid – säte ei laiene sellistele isikuandmetele, mis ei ole lepinguliste kohustuste rikkumise seisukohalt olulised. Kuna lepingulise kohustuse rikkumine ei ole isikut püsivalt negatiivselt iseloomustav fakt, siis ei tohi vaadeldavaid isikuandmeid töödelda ja edastada igavesti. Vastav säte tugineb isikuandmete kaitse üldmääruse art 6 lõike 1 punktile e, mille alusel on liikmesriikidel võimalus kehtestada seaduslik alus isikuandmete töötlemiseks, kui selle eesmärk on avalikes huvides oleva ülesande täitmine.

Võrreldes kehtiva IKS-iga on muudetud sätte pealkirja ning sättest on eemaldatud viited õigustatud huvile, kuna isikuandmete kaitse üldmääruse kohaselt ei ole liikmesriikidel võimalik õigustatud huvi iseseisvalt sisustada. Sätte pealkirja muutmise tingis asjaolu, et isiku usaldusväärsust kontrollitakse seoses võlakohustuse rikkumisega, mitte üldiselt.

Lõikesse 2 on võrreldes kehtiva IKS-iga lisatud, et keelatud on süüteo toimepanemise või selle ohvriks langemisega seonduvate andmete töötlemine enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist. Lisaks on pikendatud aega, millal võib andmeid töödelda ning ajaliseks piiriks on pandud 5 aastat.

Isikuandmete töötlemine õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel ja karistuste täideviimisel

Vastavalt üldmääruse nr 2016/679 art 2 lõike 2 punktile d ei kohaldata määrust, kui isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil. Isikuandmete töötlemisele nimetatud eesmärkidel teostatavate isikuandmete töötlemise toimingute suhtes kohaldatakse seetõttu kõnesoleva eelnõu sätteid. Eelnõu 4. peatükk sätestab isikuandmete töötlemise õiguslikud alused, mida peavad järgima õiguskaitseasutused süütegude tõkestamisel, avastamisel, menetlemisel või karistuste täideviimisel.

Isikuandmete töötlemine õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel ja karistuste täideviimisel

Vastavalt üldmääruse nr 2016/679 art 2 lõike 2 punktile d ei kohaldata määrust, kui isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil. Isikuandmete töötlemisele nimetatud eesmärkidel teostatavate isikuandmete töötlemise toimingute suhtes kohaldatakse seetõttu kõnesoleva eelnõu sätteid. Eelnõu 4. peatükk sätestab isikuandmete töötlemise õiguslikud alused, mida peavad järgima õiguskaitseasutused süütegude tõkestamisel, avastamisel, menetlemisel või karistuste täideviimisel.

§ 11. Käesoleva peatüki kohaldamine

Eelnõu § 11 kohaselt kohaldatakse uue IKS-i 4. peatükki isikuandmete töötlemisele õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel või karistuste täideviimisel. Direktiiv 2016/680 kasutab kohaldamisala piiritlemisel süütegude *tõkestamist* (*prevention*), *uurimist* (*investigation*), *avastamist* (*detection*), *vastutusele võtmist* (*prosecution*) ja *kriminaalkaristuste täitmisele pööramist* (*execution of criminal penalties*). Eesti õiguses on nii süütegude uurimine kui ka nende eest vastutusele võtmine direktiivi mõttes hõlmatud süütegude menetlemise mõistega, mistõttu kasutatakse just terminit *süütegude menetlemine*. Kuigi direktiivi 2016/680 kohaldamisala piiritlemisel kasutatakse eestikeelses tõlkes sõnastust *karistuse täitmisele pööramine* (*execution of criminal penalties*), on Eesti õigusega vastavuses *karistuse täideviimine*, mis hõlmab ka kohtuotsuse täitmisele pööramise.

IKS-i 4. peatükk on erireeglite kogum õiguskaitseasutuste jaoks ning sätestab erisused, mis arvestavad õiguskaitseasutuste tegevuse eripära. 4. peatükk kehtib ainult õiguskaitseasutuste suhtes, muud töötlejad on peatüki kohaldamisalast välistatud. Õiguskaitseasutuste puhul kehtivad omakorda teised IKS-i peatükid, arvestades, et 4. peatükis sätestatud on erinormid IKS-i teiste sätete suhtes. Üldmäärus õiguskaitseasutustele ei kohaldu, v.a juhul, kui IKS-ist ei tulene teisiti.

Vastavalt eelnõu § 11 lõikele 2 jääb seaduse 4. peatüki kohaldamisalast välja riikliku järelevalve teostamine korrakaitseseaduse § 2 lõike 4 tähenduses, kuivõrd sellisel juhul ei ole tegemist pädeva asutuse tegevusega, mis seisneks süütegude ennetamises, avastamises, uurimises, süüdistuse esitamises või avaliku julgeoleku tagamises direktiivi kohaldamisala tähenduses.

Seega kohaldatakse riikliku järelevalve teostamisel määrust 2016/679 ning eelnõu 4. peatükki tuleb kohaldada väärteomenetluse alustamisel. Riikliku järelevalve pädevusega asutuste puhul, nagu seda on näiteks Terviseamet ja Tööinspektsioon, on vaja pöörata tähelepanu eelkõige määruse ja direktiivi erinevale kohaldamisalale. Kahe akti kohaldamine eeldab nende kohaldamisala eristamist ehk eristamist riikliku järelevalve teostamise ja väärteomenetluse läbiviimise vahel. Seega tuleb isikuandmete töötlemisele riikliku järelevalve teostamisel kohaldada andmekaitse üldmäärust ning eelnõu 4. peatüki kohaldamine tuleb kõne alla siis, kui alustatakse väärteomenetlust.

Direktiivi 2016/680 ei kohaldata isikuandmete töötlemisele sellise tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse. Seega jääb direktiivi kohaldamisalast välja riikliku julgeolekuga seotud tegevus, riikliku julgeoleku küsimustega tegelevate asutuste või üksuste tegevus ning isikuandmete töötlemine liikmesriikide poolt Euroopa Liidu lepingu V jaotise 2. peatüki kohaldamisalasse kuuluva tegevuse käigus. Eestis hõlmab see julgeolekuasutusi, kelle tegevuse eesmärk on julgeolekuasutuste seaduse (JAS) § 2 lõike 1 järgi tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning koguda ja töödelda julgeolekupoliitika kujundamiseks ja riigikaitseks vajalikku teavet. JAS § 3 lõike 1 järgi kogub ja töötleb julgeolekuasutus teavet, sealhulgas isikuandmeid, kui see on vajalik tema ülesannete täitmiseks. Eelnõu 4. peatükk ei kohaldu seega JASi alusel nimetatud julgeolekuasutustele riigi julgeoleku tagamisel (JAS § 5 kohaselt on julgeolekuasutused Kaitsepolitseiamet ja Välisluureamet). Eelnõu 4. peatükk kohaldub Kaitsepolitseiameti poolt isikuandmete töötlemisele, kui seda ei tehta riigi julgeoleku tagamiseks, vaid JAS § 6 punkti 3 kohaselt kuritegude tõkestamisel ning § 6 punkti 4 alusel kuritegude kohtueelsel uurimisel. Seda põhjusel, et sellise tegevuse puhul on täidetud nii materiaalse kui ka isikulise kohaldamisala kriteeriumid, mis on direktiivi ja seega kõnealuse eelnõu 4. peatüki kohaldamise eelduseks. (Vt ka seletuskirja § 2 selgitusi.)

Eelnõu 4. peatüki kohaldamisala piiritlemiseks on eristatud isikulist ja materiaalset kohaldamisala. Eelnõu 4. peatüki sätete kohaldamiseks peavad olema täidetud kumulatiivselt nii materiaalse kui isikulise kohaldamisala kriteeriumid. Seega ei piisa eelnõu 4. peatüki sätete rakendamiseks sellest, et tegemist on pädeva asutusega, kui asutus tegutseb väljaspool materiaalses kohaldamisalas sätestatud ülesannete piire (näiteks Politsei- ja Piirivalveameti tegevus personali värbamisel). Isikulise kohaldamisala piiritlemiseks on selles peatükis võetud kasutusele õiguskaitseasutuse termin. Vastavalt eelnõu §-le 12 on õiguskaitseasutus 4. peatüki tähenduses asutus, kes on pädev seaduse alusel süütegusid tõkestama, avastama, menetlema või karistusi täide viima. Õiguskaitseasutus eelnõu 4. peatüki tähenduses on seaduses sätestatud väärtegude kohtuvälised menetlejad, nagu Finantsinspektsioon, Maanteeamet, Terviseamet, Tööinspektsioon jm. Samuti karistuse täideviimisega tegelevad asutused, nagu vanglad ja kriminaalhooldusosakonnad. Karistuse täitmisele pööramine hõlmab nii rahatrahvi ja aresti kui ka rahalise karistuse ja vangistuse täitmisele pööramist. Väärteomenetluses pöörab määratud karistuse täitmisele kas kohtuväline menetleja või maakohus (VTMS § 202), kriminaalmenetluses on karistuse täitmisele pööramine kohtu või valdkonna eest vastutava ministri käskkirjaga määratud asutuse ülesanne (KrMS §-d 414 ja 417). Üldkasuliku töö, elektroonilise valve ja ravi täideviimise eest vastutab süüdimõistetu elukohajärgne kriminaalhooldusosakond (KrMS §-d 419, 419^1, 419^2). Samuti tuleb kõnealuse peatüki sätteid kohaldada vangistuse ja aresti täideviimise korral vanglate ja arestimajade tegevusele. Õiguskaitseasutuste regulatsioon ei laiene rahalise karistuse ega trahvi täitmisele pööramisele kohtutäituri poolt.

Lisaks isikulisele kohaldamisalale tuleb 4. peatüki kohaldamisala piiritlemiseks eristada ka selle materiaalset kohaldamisala. Nimelt kohaldub eelnõu 4. peatükk üksnes osale õiguskaitseasutuse tegevustest ning seetõttu jääb 4. peatüki kohaldamisalast välja selline õiguskaitseasutuse tegevus, mis ei ole suunatud süütegude tõkestamisele, avastamisele, menetlemisele või karistuste täideviimisele. Selline on näiteks õiguskaitseasutuse haldustegevus (sh dokumendihaldus, personalitöö jt), õiguskaitseasutuste haldustegevusele kohaldub määrus nr 2016/679.

§ 12. Terminid

Eelnõu 4. peatükis kohaldatakse määruse nr 2016/679 artiklis 4 sätestatud termineid, et tagada isikuandmete valdkonda puudutavate terminite samatähenduslik kasutamine isikuandmete töötlemisega seonduva valdkonna reguleerimisel. Eriliiki isikuandmete definitsioon tuleneb üldmääruse artiklist 9 lõikest 1. Lisaks defineerib direktiiv 2016/680 artikli 3 punktis 7 pädeva asutuse, kelleks on eelnõu 4. peatüki tähenduses õiguskaitseasutus.

§ 13. Isikuandmete töötlemise põhimõtted

Eelnõu §-s 13 on sätestatud isikuandmete töötlemise põhimõtted, mis tulenevad direktiivi 2016/680 artiklist 4 ning mida tuleb järgida 4. peatüki kohaldamisalasse jääva isikuandmete töötlemise korral. Direktiivi artiklist 4 tulenevad andmetöötluse üldpõhimõtted on sarnased üldmääruse artiklis 5 sätestatuga, kuid arvestades valdkonna eripära on isikuandmete töötlemise põhimõtted sätestatud mõnevõrra leebemalt.

Eelnõu punktis 1 nimetatud põhimõtte kohaselt töödeldakse isikuandmeid seaduslikult ja õiglaselt. Selleks et isikuandmete töötlemine oleks seaduslik, peab nende töötlemine olema vajalik pädeva asutuse avalikes huvides oleva ülesande täitmiseks liidu või liikmesriigi õiguse alusel süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil (direktiivi art 4 lõike 1 punkt 1, art 8 ja direktiivi põhjenduspunkt 35). Seaduslikkuse põhimõte ei takista õiguskaitseasutustel näiteks jälitustoimingute läbiviimist ning sellised toimingud on lubatud süütegude tõkestamise, avastamise, menetlemise või karistuste täideviimise eesmärgil, kui need on seaduses ette nähtud ning kujutavad endast demokraatlikus ühiskonnas vajalikku ja proportsionaalset meedet ning nende puhul arvestatakse nõuetekohaselt asjaomase füüsilise isiku õigustatud huve.

Andmekaitses kehtiv õiglase töötlemise põhimõte on määratletud Euroopa Liidu põhiõiguste harta artiklis 47 ja Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 6 õiglase kohtumenetluse õigusest eraldiseisva põhimõttena. Direktiivi põhjenduspunkti 26 kohaselt tuleb isikuandmete töötlemisel füüsilisi isikuid teavitada nende isikuandmete töötlemisega seotud ohtudest, normidest, kaitsemeetmetest ja õigustest ning sellest, kuidas nad saavad isikuandmete töötlemisega seoses oma õigusi kasutada (vt ka eelnõu 4. peatüki 3. jagu „Andmesubjekti õigused“ ja § 44 „Andmesubjekti teavitamine isikuandmetega seotud rikkumisest“).

Eelnõu punktis 2 on sätestatud eesmärgikohasuse põhimõte, mille kohaselt kogutakse isikuandmeid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda viisil, mis on nende eesmärkidega vastuolus. Eesmärgikohasuse põhimõttest tulenevalt tohib isikuandmeid koguda süütegude tõkestamise, avastamise, menetlemise või karistuste täideviimise eesmärgil. Õiguskaitsevaldkonna puhul võib süütegude tõkestamiseks, avastamiseks, menetlemiseks ja karistuste täideviimiseks olla vaja konkreetsel eesmärgil kogutud andmeid kasutada ka muuks otstarbeks ja teises menetluses, et saada teadmisi kuritegevuse kohta ning eri avastatud süütegusid omavahel seostada. Valdkonna eripära arvestades on üsna tavapärane, et andmete kasutamise eesmärk muutub ning tekib vajadus kasutada varem kogutud andmeid ka muul eesmärgil. Sellest tulenevalt on kõnesoleva eelnõu §-s 6 sätestatud alused isikuandmete töötlemiseks muul eesmärgil. Vastavalt eelnõu § 6 lõike

1 punktile 2 võib avaliku võimu kandja isikuandmeid töödelda muul eesmärgil võrreldes sellega, mille jaoks isikuandmed on algselt kogutud, kui seda tehakse avaliku ülesande täitmiseks või avaliku võimu teostamiseks ning andmete edasine töötlemine on vajalik süütegude tõkestamiseks, avastamiseks, menetlemiseks või karistuste täideviimiseks.

Eelnõu punktis 3 on sätestatud andmete kvaliteedi põhimõte, mille kohaselt isikuandmed peavad olema piisavad ja asjakohased ning ei tohi olla ülemäärased andmetöötluse eesmärkide suhtes. Sellest tulenevalt võib isikuandmeid koguda üksnes ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. See põhimõte erineb üldmääruse art 5 lõike 1 punktis c sätestatust, mille kohaselt on isikuandmete kogumine piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt (võimalikult väheste andmete kogumise põhimõte). Direktiivi artikli 4 lg 1 punkti c kohaselt ei tohi andmed olla ülemäärased andmetöötluse eesmärkide suhtes. Tulenevalt eelnõu 4. peatüki kohaldamisala valdkonnast on see andmetöötluse põhimõte sätestatud pehmemalt, sest nii kriminaal- kui ka väärteomenetluse eri etapil ei pruugi olla teada, millised andmed on taotletava eesmärgi suhtes asjakohased ning seetõttu võib menetlejal olla tarvis koguda andmeid ulatuslikumalt, kui neid tegelikult kasutatakse. Samas tuleb arvestada, et selline andmete kogumine ei tohi olla siiski ülemäärane ning peab olema kooskõlas ka eesmärgikohasuse põhimõttega.

Eelnõu punktis 4 on sätestatud õigsuse põhimõte, mille kohaselt isikuandmed peavad olema õiged ja vajaduse korral ajakohastatud. Sellest põhimõttest tulenevalt peab andmetöötluse eesmärgi seisukohast ebaõiged isikuandmed viivitamata kustutama või parandama. Direktiivi põhjenduspunktis 30 on märgitud, et eelkõige kohtumenetluses antakse isikuandmeid sisaldavaid ütlusi, mis põhinevad füüsiliste isikute subjektiivsel ettekujutusel toimunust ning mida ei saa alati kontrollida. Seetõttu ei tohiks õigsuse nõue puudutada tunnistuse õigsust, vaid üksnes tõsiasja, et konkreetne tunnistus on antud. Õiguse põhimõte seondub eelnõu §-s 37 nimetatud isikuandmete töötlemise nõuetega ning §-s 28 nimetatud andmesubjekti õigusega nõuda isikuandmete parandamist ja kustutamist.

Eelnõu punktis 5 on sätestatud säilitamise põhimõte, mille kohaselt säilitatakse isikuandmeid kujul, mis võimaldab andmesubjekte tuvastada üksnes seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse. Seega peaks isikuandmeid säilitama piiratud aja jooksul. Varem ei olnud Eesti õiguses isikuandmete töötlemiseks säilitamise põhimõtet sellisel kujul kehtestatud. Tagamaks, et andmeid ei säilitataks vajalikust kauem, peaks vastutav töötleja kindlaks määrama andmete kustutamise tähtajad. Säilitamise põhimõte seondub eelnõu §-ga 21, kus on sätestatud isikuandmete säilitamise nõuded.

Eelnõu punktis 6 on sätestatud turvalisuse põhimõte, mille kohaselt peab isikuandmeid töötlema viisil, mis tagab nende turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustamise eest. Turvalisuse põhimõtte järgimiseks tuleks kasutada asjakohaseid tehnilisi või korralduslikke meetmeid. Andmesubjektide õiguste ja vabaduste kaitsmise vajadusest tulenevalt esineb vajadus, et isikuandmete töötlemise ajal tuleb rakendada asjakohaseid meetmeid, et tagada isikuandmete turvalisus ja eelkõige välistada andmete omavolilise töötlemise võimalus. Turvameetmete piisavus on tulenevalt tehnoloogia arenemisest ajas muutuv näitaja, mistõttu tuleb igal ajal isikuandmete töötlemisel tagada selline turvalisuse tase, mida on võimalik saavutada, arvestades tehnoloogia taset. Turvalisuse tagamiseks peaks vastutav töötleja või volitatud töötleja hindama töötlemisega seotud ohtusid ja rakendama asjaomaste ohtude leevendamiseks meetmeid, näiteks krüpteerimist. Selliste meetmetega tuleks tagada vajalik turvalisuse tase, sealhulgas konfidentsiaalsus, ning võtta arvesse teaduse ja tehnoloogia

viimast arengut, ohule vastavaid rakenduskulusid ja kaitstavate isikuandmete laadi. Andmeturbeohtusid hinnates tuleks kaaluda isikuandmete töötlemisest tulenevaid ohtusid, nagu edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhuslik või ebaseaduslik hävitamine, kaotsiminek, muutmine või loata avalikustamine või neile juurdepääs, mille tagajärjel võib eelkõige tekkida füüsiline, varaline või mittevaraline kahju. Turvalisuse põhimõttega seonduvalt tuleb tagada, et eriliiki isikuandmete suhtes kohaldataks kõrgemaid tehnilisi ja korralduslikke kaitsemeetmeid, et tagada andmesubjektide põhiõiguste ja -vabaduste maksimaalne kaitse niivõrd tundlike isikuandmete töötlemisel. Turvalisuse põhimõte seondub eelnõu 4. peatüki 6. jaoga, kus on sätestatud isikuandmete töötlemise nõuded ja isikuandmete töötlemise turvameetmed.

§ 14. Isikuandmete töötlemise seaduslikkus

Selleks et isikuandmete töötlemine oleks seaduslik, peaks nende töötlemine olema vajalik õiguskaitseasutuse avalikes huvides oleva ülesande täitmiseks seaduse alusel süütegude tõkestamise, avastamise, menetlemise või karistuse täideviimise eesmärgil. Õiguskaitseasutustele institutsiooniliselt süütegude tõkestamise, avastamise ja menetlemise eesmärgil seadusega antud ülesanne annab neile õiguse nõuda või kohustada, et füüsilised isikud vastaksid esitatud taotlustele. Seetõttu ei ole andmesubjekti nõusolek (mis on määratletud üldmääruses 2016/679) õiguslik alus isikuandmete töötlemiseks õiguskaitseasutuste poolt. Kui õiguskaitseasutus nõuab andmesubjektilt juriidilise kohustuse täitmist, puudub andmesubjektil tõeline ja vaba valikuvõimalus ning seetõttu ei saa tema reaktsiooni käsitada vabatahtliku tahteavaldusena. See ei takista aga näiteks võimalust näha ette seda, et andmesubjekt võib nõustuda oma isikuandmete töötlemisega nimetatud eesmärgil, nagu näiteks tema asukoha jälgimine elektroonilise valve kohaldamisel karistuste täideviimisel.

§ 15. Isikuandmete töötlemine algsest erineval eesmärgil

Nii direktiiv 2016/680 kui ka üldmäärus reguleerivad olukordi, kus isikuandmeid soovitakse töödelda muul eesmärgil kui see, milleks andmeid algselt koguti. Üldmääruse kohaldamisalasse jäävatele olukordadele tuleb kohaldada üldmääruse art 6 lõiget 4. Õiguskaitseasutuste poolt andmete töötlemine algsest erineval eesmärgil on sätestatud direktiivi artikli 4 lõikes 2 ning artiklis 9.

Juhul kui muul eesmärgil andmete töötlemine toimub õiguskaitseasutuste poolt, tuleb esiteks arvestada, et töötlemine võib toimuda kas täpselt sama asutuse poolt, kes andmeid algselt kogus, või ka muu õiguskaitseasutuse poolt. Igal juhul on oluline, et töötlemine peab aset leidma õiguskaitseasutuse poolt ning õiguskaitseasutuse seatud eesmärkide täitmiseks. Näiteks võib tuua olukorra, kus ühe menetluse raames kogutud andmeid soovitakse kasutada teiste menetluste tarbeks, riiklikusse DNA- või sõrmejälgede registrisse kantud andmete kasutamist kriminaalmenetluses jne. Igal juhul peab õiguskaitseasutuse volitus töödelda andmeid tulenema Eesti või EL-i õigusaktist (näiteks kriminaalmenetluse seadustik, politsei ja piirivalve seadus jt) ning tagama peab proportsionaalsuse põhimõtte järgimise. Siinkohal on näiteks kriminaalmenetluse seadustiku § 99^2, mis annab võimaluse kasutada raskete kuritegude uurimisel DNA- ja sõrmejäljeandmeid, mis koguti muul eesmärgil. Edasise töötlemise alused peavad tulenema seadusest, mitte sellest madalamal seisvast õigusaktist, sest andmete kasutamisest tulenev põhiõiguste riive on väga suur.

Täiendavalt tuleb eristada olukordi, kus isikuandmete edasine töötlemine toimub eesmärgil, mis ei ole seotud õiguskaitseasutuste tegevusega. Sellises olukorras peab töötlemine olema selgelt lubatud Eesti või EL-i õigusega ning sellise töötlemise suhtes tuleb kohaldada üldmäärust. Näiteks saab selline olukord aset leida siis, kui kriminaalmenetluse raames kogutud andmeid soovitakse kasutada haldus- või distsiplinaarmenetluses jt.

Lisaks on sätestatud, et kui õiguskaitseasutusele on antud ka muud pädevused kui need, mis on hõlmatud § 11 lõikega 1 (süütegude uurimine, avastamine, menetlemine, süüdistuse esitamine ja kriminaalkaristuse täitmisele pööramine), siis tuleb sellisele töötlemisele kohaldada üldmäärust või Eesti õigust (kui töötlemine ei kuulu EL-i õiguse kohaldamisalasse). Näiteks kui PPA täidab lisaks § 11 lõikes 1 nimetatud ülesannetele ka migratsiooniga seotud ülesandeid, tuleb nende ülesannete täitmisele kohaldada üldmäärust.

§ 16. Isikuandmete säilitamine

Erinevalt kehtivast IKS-ist on eelnõus kavandatuga sätestatud isikuandmete kindla säilitamisperioodi nõue. See nõue tuleneb direktiivi art 4 lg 1 punktist e ning artiklist 5. Vastavalt direktiivi põhjenduspunktile 26 peaks vastutav töötleja selle tagamiseks, et andmeid ei säilitataks vajalikust kauem, kindlaks määrama tähtajad andmete kustutamiseks või korrapäraseks läbivaatamiseks. Isikuandmeid tohib säilitada kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik õigusaktis sätestatud eesmärgi saavutamiseks. Isikuandmete säilitamise tähtaeg on üldjuhul sätestatud seaduses, mille puhul vastutaval töötlejal ei ole võimalik eraldi säilitamise tähtaega kehtestada ning tuleb järgida seaduses sätestatut. Olukorras, kus seaduses säilitamise tähtaega ei ole kehtestatud, peab vastutav töötleja isikuandmete töötlemisel tagama, et kehtestab ka isikuandmete säilitamise tähtaja. Isikuandmeid ei ole lubatud säilitada vajalikust kauem, mistõttu tuleb need pärast säilitamise tähtaja lõppemist jäädavalt kustutada. Tulenevalt eelnõu § 21 lõikest 1 määrab vastutav töötleja kindlaks töödeldavate isikuandmete säilitamise tähtaja, mida vastavalt lõikele 2 võib vastutav töötleja põhjendatud juhul pikendada. Seega ei pikene isikuandmete säilitamise tähtaeg automaatselt, vaid nende säilitamise pikendamine peab olema põhjendatud. Säilitamisperioodi pikendamist peavad toetama piisavad ja asjakohased põhjused.

Isikuandmete säilitamise tähtaja kindlaksmääramisel tuleb arvesse võtta isikuandmete töötlemise eesmärki ja selle vajadust kooskõlas proportsionaalsuse põhimõttega. Isikuandmete säilitamise tähtaja lõppemisel kustutab vastutav töötleja isikuandmed jäädavalt. Isikuandmete kustutamise all mõistetakse sisuliselt andmete hävitamist ehk andmed tuleb andmetöötlusest kõrvaldada sellisel viisil, et nende hilisem taastamine ei oleks tehniliselt võimalik. Tuleb arvestada, et andmete arhiveerimine on samuti töötlemine, mistõttu ei asenda andmete arhiveerimine nende kustutamist. Eelnõu § 16 lõikes 1 sätestatud nõue välistab võimaluse säilitada isikuandmeid määramata aja jooksul.

Isikuandmete säilitamise tähtaeg peab olema kindlaks määratud ka andmesubjekti õiguste tagamiseks. Tulenevalt eelnõu § 22 lg 1 punktist 3 peab vastutav töötleja seaduses sätestatud andmesubjekti teavitamise kohustuse korral teavitama andmesubjekti isikuandmete säilitamise tähtajast või säilitamise tähtaja määramise alustest. Seega on andmesubjektil õigus teada, millise perioodi vältel tema kohta käivaid isikuandmeid säilitatakse.

§ 17. Andmesubjektide eri kategooriate eristamine

Eelnõu §-s 22 on sätestatud direktiivi artiklist 6 tulenev põhimõte, mille kohaselt peab andmesubjekte selgelt eristama eri kategooriate kaupa. Tegemist on põhimõttega, mida varem isikuandmete kaitse seaduses või menetlusseadustikes ei olnud kehtestatud. Direktiivi põhjenduspunkti 31 kohaselt on kriminaalasjades tehtava õigusalase koostöö ja politseikoostöö käigus isikuandmete töötlemise puhul olemuslik, et töödeldakse eri kategooriatesse kuuluvate andmesubjektide isikuandmeid. Seetõttu, kui see on asjakohane, tuleks sellises ulatuses nagu võimalik selgelt eristada selliste andmesubjektide eri kategooriate isikuandmeid, nagu:
1) kahtlusaluse;
2) süüteos süüdi mõistetud isikute;
3) süüteo ohvrite ning
4) muude isikute, nagu tunnistajad ja asjakohast teavet omavad isikud, ning kahtlustatavate ja süüdimõistetute kontaktisikute ja kaasosaliste andmed.

Eesti õiguses ei olnud nõuet eristada andmesubjektide kategooriaid varem kehtestatud. Andmesubjektide eri kategooriatena on eelnõu §-s 17 nimetatud kahtlustatavad, süüdistatavad, kannatanud, kriminaalhooldusalused isikud, kinnipeetavaid, arstialuseid ning tunnistajad, kes on KrMS § 16 lg 2 kohaselt menetlusosalised. Lisaks nimetab väärteomenetluse seadustiku § 16 menetlusosalisena menetlusalust isikut. Sellest tulenevalt on vastutaval töötlejal kohustus eristada asjakohasel juhul isikuandmete töötlemisel andmesubjektide eri kategooriatena menetlusalused isikud, kahtlustatavad, süüdistatavad, kannatanud ning tunnistajad juhul, kui see on võimalik. Nimekiri on jäetud lahtiseks, kuivõrd oluline on tagada, et kõik isikuandmete töötlemises nimetatud isikud oleksid selgelt eristatavad. Vastutav töötleja peab seega kasutusele võtma meetmeid, mis võimaldavad andmesubjekte eristada, ning näiteks andmetöötlustoimikutes ja registrites selgelt märkima, millist rolli andmesubjekt menetluses täidab.

§ 18. Hinnangutel põhinevate isikuandmete eristamine

Direktiivi art 7 lõikest 1 tuleneb kohustus eristada faktidel põhinevaid isikuandmeid nii palju kui võimalik isiklikel hinnangutel põhinevatest isikuandmetest. Direktiivi põhjenduspunkti 47 kohaselt peaks füüsilisel isikul olema õigus teda käsitlevate ebaõigete isikuandmete parandamisele, eelkõige juhul, kui tegemist on faktiliste andmetega, ja kustutamisele, kui selliste andmete töötlemine rikub kõnesolevat direktiivi. Siiski ei tohiks andmete parandamise õigus mõjutada näiteks tunnistaja ütluse sisu. Seega on nõue eristada hinnangutel põhinevaid isikuandmeid seotud ka andmesubjekti õigusega nõuda teda käsitlevate ebaõigete isikuandmete parandamist. Andmesubjekti õigus nõuda andmete parandamist puudutab just faktidel põhinevaid isikuandmeid. Näiteks on raske ette kujutada olukorda, kus kahtlustatav nõuaks tema kohta käivate andmete parandamist kriminaaltoimikus, mis puudutab tunnistaja antud ütlusi. Seetõttu on vaja eristada ka faktidel ja hinnangutel põhinevaid isikuandmeid, et oleks võimalik sisustada andmesubjekti õigust nõuda isikuandmete parandamist. Näiteks on tunnistaja ülekuulamisprotokollis KrMS § 74 alusel selgelt eristatavad faktilised ja hinnangutel põhinevad isikuandmed. Nimelt KrMS § 74 lõike 1 punkti 1 alusel on tunnistaja nimi, isikukood, kodakondsus, haridus, elu- ja töökoht või õppeasutuse nimetus faktidel põhinevad isikuandmed, mille õigsust on võimalik kontrollida. Samas on KrMS § 74 lõike 1 punktis 3 nimetatud tunnistaja ütlused sellised, kus sisalduvad hinnangutel põhinevad isikuandmed.

§ 19. Eriliiki isikuandmete töötlemise erisused

Eriliiki isikuandmete definitsioon tuleneb üldmääruse artiklist 9. Sama definitsiooni kohaldatakse ka õiguskaitseasutuste poolt andmete töötlemisele. Eriliiki isikuandmed, mida on keelatud töödelda, on isikuandmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, samuti on keelatud töödelda geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. Üldmääruse art 9 lg 1 kohaselt on eriliiki isikuandmete töötlemine üldjuhul keelatud ning töötlemine on lubatud ainult erandlikes olukordades (üldmääruse art 9 lg 2). Arvestades direktiivi 2016/680 kohaldamisala ja õiguskaitseasutuste tegevuse eripära, ei ole sellise keelu kohaldamine võimalik. Seetõttu näeb direktiivi art 10 ette teistsugust lähenemist. Nimelt sätestatakse, et eriliiki isikuandmete töötlemine on lubatud ainult juhul, kui esineb üks järgmistest alustest:
1) töötlemise lubatavus on sätestatud õigusaktis;
2) töötlemine on vajalik andmesubjekti või teise füüsilise isiku eluliste huvide kaitseks või
3) töödeldakse isikuandmeid, mille andmesubjekt on ise ilmselgelt avalikustanud.

Selline lähenemine võimaldab õiguskaitseasutustel täita ülesanded, mis sageli võivad hõlmata eriliiki isikuandmete töötlemist, näiteks seksuaalkuritegude menetlemine, kinnipeetava terviseseisundi hindamine ja kontroll, DNA- ja sõrmejäljeandmete kasutamine menetluses jt.

§ 20. Automatiseeritud töötlemine

Eelnõu § 19 lõike 1 kohaselt on keelatud andmetöötlussüsteemi (andmete töötlemiseks loodud süsteem, nt algoritmidel põhinevaid töötlemistoiminguid teostav infosüsteem) poolt selliste otsuste tegemine, mis toob andmesubjektile kaasa õiguslikke tagajärgi või mõjutab teda märkimisväärselt muul viisil. Direktiivi põhjenduspunkti 38 kohaselt peaks andmesubjektil olema õigus nõuda, et tema suhtes ei tehta üksnes isikuandmete automatiseeritud töötlemisele toetuvat isiklike aspektide hindamisel põhinevat otsust, millel on teda puudutavad negatiivsed õiguslikud tagajärjed või mis teda märkimisväärselt mõjutavad. Selliseks negatiivseks mõjuks isikule võib olla näiteks kahtlustuse esitamine automatiseeritud töötlemise tulemusena saadud profiili põhjal või isikule karistuse määramine lähtuvalt automatiseeritud töötlemisel saadud isikukirjeldusest jt. Igal juhul tuleks sellise töötlemise korral kohaldada sobivaid kaitsemeetmeid, mis muu hulgas hõlmavad andmesubjektile konkreetse teabe andmist ja õigust otsesele isiklikule kontaktile, eelkõige õigust väljendada oma seisukohta, õigust saada selgitust otsuse kohta, mis tehti pärast sellist hindamist, ja õigust otsust vaidlustada. Ühe sobiva kaitsemeetmena on ette nähtud eelnõu § 19 lõikes 2 andmesubjekti õigus esitada vastutavale töötlejale vastuväiteid oma õigustatud huvi kaitseks. Selline andmesubjekti õigus on näiteks tagatud KrMS §-s 228 sätestatud võimalusega kaevata uurimisasutuse ja prokuratuuri tegevuse peale. Nimelt on KrMS § 228 järgi menetlusosalisel ja menetlusvälisel isikul õigus esitada prokuratuurile kaebus uurimisasutuse menetlustoimingu või määruse peale. See õigus tagab ka andmesubjektile võimaluse oma õigustatud huve kaitsta, kui ta leiab, et tema õigusi on automatiseeritud otsuse tegemisega rikutud.

§ 21. Andmesubjektile kättesaadavaks tehtav teave

Vastavalt eelnõu § 21 lõikele 1 on vastutav töötleja kohustatud avalikustama punktides 1–5 nimetatud teabe. Tegemist on andmesubjektile kättesaadavaks tehtava teabega, mis peaks võimaldama andmesubjektil oma õigusi teostada. See teave võimaldab andmesubjektil tutvuda, mis eesmärgil võib vastutav töötleja isikuandmeid töödelda ning milline on andmesubjekti õiguste teostamise kord. Samuti peavad olema andmesubjektile lihtsasti kättesaadavad andmekaitsespetsialisti, vastutava töötleja ning Andmekaitse Inspektsiooni kontaktandmed. Selline teave võib olla avalikustatud näiteks vastutava töötleja veebisaidil või muul andmesubjektile hõlpsasti ligipääsetavas asukohas. Selleks et andmesubjektil oleks võimalik oma õigusi tõhusalt teostada, peaks teave olema ka kergesti arusaadav ning selgelt ja lihtsalt sõnastatud.

§ 22. Andmesubjekti teavitamisel antav teave

Eelnõu §-s 22 on ette nähtud kohustus anda andmesubjektile lõike 1 punktides 1–5 nimetatud teave sellisel juhul, kui seaduses on sätestatud kohustus teavitada andmesubjekti tema isikuandmete töötlemisest. Tegemist on andmesubjekti aktiivse teavitamise kohustusega, mida peab täitma vastutav töötleja ning milleks ei ole vaja andmesubjekti taotlust. Selliseks olukorraks on näiteks KrMS §-s 126^{13} sätestatud jälitustoimingust teavitamine, mille kohaselt teavitatakse isikut, kelle suhtes jälitustoiming tehti, ning isikut, kelle perekonna- või eraelu puutumatust jälitustoiminguga oluliselt riivati ja kes on menetluse käigus tuvastatud. Isiku teavitamisel tuleb sellisel juhul anda andmesubjektile ka lõike 1 punktides 1–5 nimetatud teave, et andmesubjektil oleks võimalik oma õigusi teostada.

Vastuvõtjate kategooriateks võib eelnõu § 22 lg 1 p 4 kohaselt olla näiteks: välisriikide pädevad asutused, kellele andmed edastatakse vastastikuse õigusabi raames, julgeolekuasutused, asutused, kes teostavad isiku suhtes tausta- või julgeolekukontrolli jt.

Eelnõu § 22 lõikes 2 on ette nähtud teabe andmise piiramise õigus, mille kohaselt võib teabe andmesubjektile esitada hiljem, piirata selle esitamist või jätta selle esitamata punktides 1–5 sätestatud juhtudel. Andmesubjekti õiguste piiramisel tuleb kaaluda andmesubjekti huve ning teiselt poolt punktide 1–5 alusel kaitstavaid huve, milleks on ametlike päringute tegemine, uurimine ja menetlemine, süütegude tõkestamine, avastamine, menetlemine või karistuste täideviimine, teise isiku õigused ja vabadused, riiklik julgeolek ning avalik kord.

§ 23. Andmesubjekti õigus saada teavet ja enda kohta käivaid isikuandmeid

Sätte eesmärk on tagada, et füüsilisel isikul oleks võimalik teada, kas tema isikuandmeid töödeldakse, ja selleks et kontrollida sellise töötlemise seaduslikkust, õigus tutvuda andmetega, mis on tema kohta kogutud. Füüsiliste isikute kaitse isikuandmete töötlemisel on käsitatav põhiõigusena tulenevalt Euroopa Liidu põhiõiguse harta artikli 8 lõikest 1, mis sätestab, et igaühel on õigus oma isikuandmete kaitsele. Selle põhiõiguse lahutamatuks osaks on andmesubjekti õigus tutvuda isikuandmetega.

Vastavalt § 23 lõikele 1 on andmesubjektil õigus esmalt saada vastutavalt töötlejalt kinnitus selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse. Juhul kui isikuandmeid töödeldakse, sätestab § 22 lõige 2, millise teabe on vastutav töötleja kohustatud andmesubjekti soovil temale teatavaks tegema. Igal andmesubjektil peaks olema õigus teada

isikuandmete töötlemise eesmärke, töödeldavate isikuandmete kategooriaid (terviseandmed, kontaktandmed, andmed vanemate kohta jt), töötlemise ajavahemikku ja andmete vastuvõtjaid, sealhulgas kolmandas riigis, ning saada eelneva kohta teavet. Kui sellise teavitamise käigus antakse teavet isikuandmete päritolu kohta, et tohiks selline teave paljastada füüsiliste isikute identiteeti ega eelkõige konfidentsiaalseid allikaid. Kõnealuse õiguse tagamiseks piisab, kui andmesubjektil on olemas arusaadaval kujul nimetatud andmete täielik kokkuvõte ehk andmed kujul, mis võimaldab tal saada nendest andmetest teadlikuks ning kontrollida, et need on õiged ja neid töödeldakse isikuandmete kaitse seaduse kohaselt. Sellise kokkuvõtte võib esitada näiteks töödeldavate isikuandmete koopiana.

Juurdepääs andmetele, mis sisalduvad kriminaaltoimikus, on reguleeritud KrMS-i sätetega, mis reguleerivad juurdepääsu kriminaaltoimikule. Kriminaaltoimik on KrMS § 160^1 kohaselt kriminaalmenetluses kogutud dokumentide kogum, seega sisaldab kriminaaltoimik nii kriminaalmenetluses töödeldud andmeid kui ka andmetöötlust puudutavat teavet. KrMS §-de 224 ja 224^1 kohaselt on kahtlustataval, süüdistataval, kaitsjal, kannatanul ning tsiviilkostjal õigus tutvuda kriminaaltoimikuga. KrMSi kohaselt on selgelt piiritletud isikute ring, kellel on õigus toimikuga tutvuda. Samas võib toimikus sisalduda märkimisväärsel hulgal ka infot teiste isikute kohta, kellele aga ei ole võimaldatud juurdepääs toimikule ja sellest tulenevalt ka nende kohta kogutud isikuandmetele. Näiteks võib toimikus olla ulatuslikult teavet tunnistajate ja menetlusosaliste pereliikmete või tuttavate kohta, nende eraelu puudutavaid andmeid ja muu privaatsusõiguse kaitsealasse jäävat teavet. Siiski ei teki nendel isikutel toimikuga tutvumise õigust, kuivõrd see võib kahjustada kriminaalmenetlust. Kohtueelse menetluse andmete avaldamise tingimused on sätestatud KrMS §-s 214, mille lõike 1 kohaselt võib kohtueelse menetluse andmeid avaldada üksnes prokuratuuri loal ja tema määratud ulatuses ning paragrahvis 2 sätestatud tingimustel. Nimetatud olukord on vastavuses ka direktiivi 2016/680 artikliga 18, mille kohaselt võivad liikmesriigid ette näha, et kui isikuandmed sisalduvad kohtuotsuses, karistusregistris või kriminaaluurimise ja -menetluse käigus töödeldavas toimikus, teostatakse andmesubjekti õigusi vastavalt liikmesriigi õigusele.

Tulenevalt valdkonna eripärast on andmesubjekti õiguste teostamine piiratud ning vastutav töötleja võib eelnõu § 23 lõikes 1 nimetatud teabe andmesubjektile esitada hiljem, piirata selle esitamist või keelduda selle väljastamisest, kui see võib takistada või kahjustada süüteo tõkestamist, avastamist, menetlemist või karistuste täideviimist, kahjustada teise isiku õigusi ja vabadusi ning juhul, kui teabe avaldamine andmesubjektile võib kahjustada riiklikku julgeolekut või avaliku korra kaitset. Siiski peaks vastutav töötleja iga konkreetse juhtumi puhul eraldi ja individuaalselt hindama, kas isikuandmetega tutvumise õigust tuleks osaliselt või täielikult piirata, kui selline andmesubjekti õiguste piiramine on proportsionaalne.

Isikuandmetega tutvumisest keeldumise või selle piiramise korral tuleks andmesubjekti sellest teavitada ning seda põhjendada. Vastav põhjendus peaks sisaldama nii otsuse faktilisi kui ka õiguslikke aluseid. Juhul kui selliste põhjenduste andmine kahjustaks mõnda lõikes 2 nimetatud eesmärki, võib vastutav töötleja jätta põhjendused esitamata. Siiski tuleb teabe andmise piiramise või keeldumise otsuse faktilised ja õiguslikud alused vastutaval töötlejal dokumenteerida, et vajaduse korral teha kõnealune teave kättesaadavaks Andmekaitse Inspektsioonile.

§ 24. Andmesubjekti õigus nõuda isikuandmete parandamist ja kustutamist

Eelnõu § 24 sätestab andmesubjekti õiguse nõuda isikuandmete parandamist ja kustutamist. Andmesubjektil on õigus nõuda teda puudutavate ebaõigete isikuandmete parandamist, eelkõige juhul, kui tegemist on faktidel põhinevate andmetega. Siiski ei tohiks andmete parandamise õigus mõjutada näiteks tunnistaja ütluse sisu ehk hinnangutel põhinevaid isikuandmeid. Asjakohasel juhul peaks andmesubjektil olema õigus nõuda mittetäielike isikuandmete täiendamist. Näiteks kui tunnistaja ülekuulamise protokolli on lisatud andmesubjekti aadress või isikukood valesti, peab andmesubjekt saama taotleda andmete parandamist.

Vastavalt eelnõu § 24 lõikele 3 on andmesubjektil õigus nõuda isikuandmete kustutamist, kui isikuandmete töötlemine ei ole seaduse alusel lubatud või rikub isikuandmete töötlemise põhimõtteid või kui kustutamine on vajalik vastutava töötleja seaduses sätestatud kohustuse täitmiseks. See säte tähendab, et andmesubjektil on võimalik nõuda andmete kustutamist, kui selline kustutamine on vajalik vastutava töötleja suhtes kehtiva õigusliku kohustuse täitmiseks (näiteks on kohtuotsusega kohustatud andmeid kustutama, vt nt KrMS § 206 lg 3^1).

Isikuandmete kustutamise asemel piirab vastutav töötleja nende töötlemist (eelnõu § 24 lg-d 4 ja 5) juhul, kui andmesubjekt vaidlustab isikuandmete õigsuse ning nende õigsust või ebaõigsust ei ole võimalik kindlaks teha või kui isikuandmeid tuleb säilitada tõendamise eesmärgil. Piiratud isikuandmeid tuleks sellisel juhul töödelda üksnes sel eesmärgil, mis takistas nende kustutamist. Isikuandmete töötlemise piiramise meetodid võivad muu hulgas hõlmata valitud andmete ümberpaigutamist teise töötlemissüsteemi, näiteks arhiveerimise eesmärgil, või valitud andmete muutmist kättesaamatuks. Automatiseeritud andmete kogumites tuleks isikuandmete töötlemise piiramine tagada üldjuhul tehniliste vahenditega. Asjaolu, et isikuandmete töötlemine on piiratud, tuleks süsteemis esitada nii, et isikuandmete töötlemisele seatud piirangu olemasolu oleks selge. Isikuandmete parandamisest, kustutamisest ja nende töötlemise piiramisest tuleks teavitada vastuvõtjaid, kellele isikuandmed on avaldatud, ning pädevaid asutusi, kellelt ebaõiged andmed pärinevad. Samuti peaksid vastutavad töötlejad hoiduma selliste andmete edasisest levitamisest. Vastutav töötleja peab teavitama andmesubjekti piirangu kõrvaldamisest, kui piirangu kehtestamine tulenes asjaolust, et isikuandmete õigsust ei olnud võimalik kindlaks teha. Sellisel juhul peaks vastutav töötleja teavitama tema poole pöördunud andmesubjektile piirangu eemaldamisest ning järgmistest sammudest, st kas vastutav töötleja kustutab andmeid vastavalt andmesubjekti taotlusele või keeldub nende kustutamisest.

Isikuandmete kustutamise piirangud tulenevad direktiivi 2016/680 art 16 lõikest 3, mis annab ammendava loetelu juhtudest, millal kustutamise saab asendada töötlemise piiramisega.

Õigus isikuandmete kaitsele on põhiõigus ning seega peavad õiguskaitseasutused oma tegevuses arvestama isikuandmete kaitse põhimõtete ja reeglitega. Nõue isikuandmeid kustutada on kehtestatud ainult juhtudeks, kui töötlemine on vastuolus isikuandmete töötlemise põhimõtetega (nt isikuandmete säilitamistähtaeg on möödunud, puudub seaduslik alus isikuandmete töötlemiseks või on andmete töötlemine selgelt keelatud, nt eriliiki isikuandmete puhul). Asjaolu, et isikuandmed võivad olla vajalikud asutuse ülesannete täitmiseks, ei anna alust rikkuda isikuandmete kaitse nõudeid.

Kui vastutav töötleja keeldub isikuandmete parandamisest, kustutamisest või nende töötlemise piiramisest, teavitab vastutav töötleja andmesubjekti viivitamata selle põhjustest. Vastutav töötleja võib jätta põhjendused esitamata, kui sellise teabe andmine takistaks või kahjustaks süüteo tõkestamist, avastamist, menetlemist või karistuste täideviimist, kahjustaks

teise isiku õigusi ja vabadusi või kahjustaks avalikku korda või riiklikku julgeolekut. Juhul kui vastutav töötleja teavitab andmesubjekti isikuandmete parandamisest või nende kustutamisest keeldumisest, teavitab ta ka õigusest pöörduda otsuse vaidlustamiseks Andmekaitse Inspektsiooni või kohtu poole.

§ 25. Vastutava töötleja kohustus teavitada isikuandmete parandamisest, kustutamisest ja nende töötlemise piiramisest

Eelnõu § 25 sätestab täiendavalt, millised on vastutava töötleja kohustused, kui ta parandab või kustutab isikuandmeid või piirab nende töötlemist vastavalt §-le 24. Sellisel juhul peab vastutav töötleja teavitama sellest pädevat asutust, kellelt isikuandmed saadi, et kõnealusel asutusel oleks samuti võimalik parandada või kustutada nende vastutuse alla kuuluvad isikuandmed või piirata nende töötlemist. Samuti on vastutav töötleja kohustatud teavitama isikuandmete vastuvõtjaid, kui selliseid isikuandmeid on edastatud. Vastuvõtja definitsioon on antud üldmääruse § 4 punktis 9 ja direktiivi § 3 punktis 10. Vastuvõtjateks ei loeta avaliku sektori asutusi, kes võivad kooskõlas liikmesriigi õigusega saada isikuandmeid seoses konkreetse päringuga; nimetatud avaliku sektori asutused töötlevad kõnealuseid isikuandmeid kooskõlas asjaomaste andmekaitsenormidega vastavalt töötlemise eesmärkidele

§ 26. Andmesubjekti õiguste teostamise kord

Eelnõu §-s 26 on sätestatud üldine andmesubjekti õiguste teostamise kord, millest tuleb lähtuda andmesubjekti taotlustele vastamisel ja nende lahendamisel, sealhulgas andmesubjektile sätestatud õiguste kasutamisel. Selleks et andmesubjektil oleks võimalik oma õigusi tõhusalt kasutada, peab vastutav töötleja vastama andmesubjekti taotlustele kokkuvõtlikus, arusaadavas ja hõlpsasti kättesaadavas vormis, kasutades selget ja lihtsat sõnastust. Võimaluse korral vastatakse andmesubjekti taotlusele tema soovitud viisil. Taotluse täitmiseks kaasnevate mõistlike kulude hüvitamist on vastutaval töötlejal võimalik küsida juhul, kui andmesubjekti taotlused on põhjendamatud või ülemäärased. Vastutav töötleja on iga taotluse puhul kohustatud hindama, kas taotlus on selgelt põhjendamatu või ülemäärane. Eelkõige on andmesubjekti taotlused põhjendamatud või ülemäärased, kui tegemist on korduva taotlusega. Sellisel juhul võib vastutav töötleja keelduda andmesubjekti taotletud meetmete võtmisest. Mõistlike kulude hüvitamiseks tuleb lähtuda seaduses, eelkõige avaliku teabe seaduses (AvTS) sätestatud teabenõude täitmise kulude katmise korrast.

§ 27. Andmesubjekti õigus pöörduda Andmekaitse Inspektsiooni poole

Andmesubjektil on õigus pöörduda Andmekaitse Inspektsiooni poole ning sellise õiguse tagamise eesmärk on saavutada võimalikult kiire ja andmesubjekti vähem koormav, kuid samas tõhus menetlus. Kui andmesubjekt on pöördunud kaebusega Andmekaitse Inspektsiooni poole, teavitab Andmekaitse Inspektsioon tema kaebuse alusel tehtud otsusest ning õigusest pöörduda Andmekaitse Inspektsiooni otsuse vaidlustamiseks kohtusse.

Lisaks on andmesubjektil eelnõu § 27 lõike 2 kohaselt õigus, et Andmekaitse Inspektsioon teavitaks teda haldusjärelevalve käigu tulemusest ehk otsusest, millele Andmekaiste Inspektsioon andmesubjekti taotluse lahendamisel jõudis.

Eelnõu § 27 lõike 3 kohaselt suunab Andmekaitse Inspektsioon andmesubjekti oma kaebuse esitamiseks teise Euroopa Liidu liikmesriigi pädeva järelevalveasutuse poole, kui kaebust on pädev lahendama teise liikmesriigi pädev järelevalveasutus. Sätte eesmärk on seotud andmesubjekti õigusega esitada kaebus ühele järelevalveasutusele, mistõttu peab Andmekaitse Inspektsioon tagama selle, et andmesubjektil on võimalus esitada oma kaebus õigele pädevale järelevalveasutusele.

§ 28. Vastutav ja volitatud töötleja

Eelnõu § 28 lõige 1 sätestab vastutava töötleja üldised kohustused, mis on seotud vastutava töötleja olemusega. Nimelt määrab vastutav töötleja kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Seetõttu on vastutava töötleja kohustus rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada isikuandmete töötlemise nõuete täitmine isikuandmete töötlemisel, ning vajaduse korral peab ta tõendama selliste nõuete täitmist. Nimetatud põhimõte tuleneb direktiivi 2016/680 art 4 lõikest 4 ning art 19.

Volitatud töötleja töötleb isikuandmeid vastutava töötleja nimel, mistõttu on eelnõu § 28 lõikes 2 sätestatud, et vastutav töötleja annab volitatud töötlejale kohustuslikke juhiseid isikuandmete töötlemiseks ja vastutab selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. Volitatud töötleja määramise õigus on üksnes vastutaval töötlejal, kellel lasub vastutus ka töötlemise nõuetekohase korraldamise eest, mistõttu volitatud töötlejate määramisel peab vastutav töötleja tagama, et volitatud töötleja suudab tagada isikuandmete töötlemisel isikuandmete kaitse piisava taseme ja vastavuse seaduse nõuetele.

Eelnõu § 28 lõikes 4 on üldine põhimõte, et volitatud töötleja võib isikuandmete töötlemise edasi volitada üksnes seaduse, seaduse alusel antud muu õigusakti või vastutava töötleja kirjalikul loal ning tingimusel, et ei ületata volitatud töötlejale antud volituste ulatust. Kirjaliku loa alusel antud volituse korral peab volitatud töötleja teavitama vastutavat töötlejat alati teiste volitatud töötlejate lisamisest või asendamisest. Vastutav töötleja võib sellisel juhul esitada selliste muudatuste suhtes vastuväiteid. Sellisteks olukordadeks võib olla näiteks tõlgi või asjatundja kaasamine või muule isikule isikuandmete töötlemise edasivolitamine. Üldjuhul peaks selline töötlemine toimuma seaduse või seaduse alusel antud õigusakti alusel. Siiski ei saa välistada, et teatud olukorras võib tekkida vajadus kaasata ka teisi töötlejaid, näiteks tõlki, kellega sõlmitakse leping.

§ 29. Volitatud töötleja määramine ja kohustused

Eelnõu § 29 reguleerib volitatud töötleja määramise reegleid ja volitatud töötleja kohustusi.

§ 30. Kaasvastutavad töötlejad

Eelnõu §-s 30 on sätestatud kaasvastutavate töötlejate mõiste ning vastutavate töötlejate vastutuse määramise kord sellises olukorras. Mitu vastutavat töötlejat võivad olla kaasvastutavad töötlejad juhul, kui nad määravad ühiselt kindlaks isikuandmete töötlemise eesmärgid ja vahendid. See tähendab, et mõlemad vastutavad töötlejad määravad võrdsetel alustel isikuandmete töötlemise eesmärgid ning selle jaoks eraldatavad vahendid määratakse samuti ühiselt, näiteks ühisest eelarvest. Seda ei saa siiski samastada olukorraga, kus mitu

isikuandmete töötlejat jagavad näiteks ühte andmebaasi. Kaasvastutavate töötlejate puhul on oluline määrata vastutusvaldkondade selge jaotumine, tehes seda kaasvastutavate töötlejate vahelise kokkuleppega.

§ 31. Isikuandmete töötlemine vastutava ja volitatud töötleja nimel

Eelnõu § 31 reguleerib olukordi, kus töötlemine toimub vastutava või volitatud töötleja nimel. Vastutavaks või volitatud töötlejaks on õiguskaitseasutus või muu asutus, kuid õiguskaitseasutuse nimel töötlevad isikuandmeid konkreetsed füüsilised isikud, kes isikuandmeid töödeldes täidavad oma töö- või teenistusülesandeid. Eelnõu § 31 sätestab reeglid, mida tuleb arvestada vastutava või volitatud töötleja nimel andmete töötlemisel.

§ 32. Lõimitud andmekaitse ja vaikimisi andmekaitse

Eelnõu §-s 32 on sätestatud kaks andmekaitse põhilist põhimõtet, milleks on lõimitud ja vaikimisi andmekaitse. Lõimitud andmekaitse põhimõtte kohaselt peab vastutav töötleja rakendama teaduse ja tehnoloogia viimaseid saavutusi ja tegema vajalikke kulutusi. Samuti peab vastutav töötleja isikuandmete töötlemisvahendite kindlaksmääramisel võtma arvesse isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke. Lisaks peab vastatav töötleja isikuandmete töötlemise ajal võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonüümimine, mis on vajalikud andmekaitse põhimõtete tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse. Nimetatud meetmed on vajalikud, et täita isikuandmete töötlemisele kohaldatavaid nõudeid ja kaitsta andmesubjektide õigusi.

Nimelt ei ole andmekaitse põhimõtete rakendamine ainult seaduses sätestatud nõuete järgimine, vaid isikuandmete töötlejad peavad igapäevaselt jälgima ka tehnoloogia arengusuundi, lisanduvaid uusi tooteid ja teenuseid. Lõimitud andmekaitse printsiipe võib rakendada igat tüüpi isikuandmete puhul. Rangemat tähelepanu nõuavad eriliiki isikuandmed, nagu näiteks inimese terviseandmed. Lõimitud andmekaitset iseloomustavad pigem ennetavad kui tagajärgedega tegelevad meetmed. Lõimitud andmekaitse põhimõtte rakendamine peaks ette nägema ja hoidma ära eraelu riivamise. Samuti peaks andmekaitse olema juba süsteemi vaikimisi sisse ehitatud ning olema selle süsteemi ülesehituse osa.

Vaikimisi andmekaitse põhimõtte kohaselt peab vastutav töötleja rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, millega tagatakse, et vaikimisi töödeldakse ainult isikuandmeid, mis on vajalikud töötlemise iga konkreetse eesmärgi saavutamiseks. Nimetatud kohustus kehtib kogutud isikuandmete hulga, töötlemise ulatuse, säilitamise tähtaja ja kättesaadavuse suhtes. Eelkõige tagatakse selliste meetmetega, et isikuandmeid ei tehta vaikimisi kättesaadavaks määramata füüsiliste isikute ringile ilma asjaomase isiku sekkumiseta.

§ 33. Isikuandmete töötlemise nõuded

Eelnõu §-s 33 on sätestatud isikuandmete töötlemise üldised nõuded, mida vastutav ja volitatud töötleja peavad isikuandmete töötlemisel täitma. Kehtiva IKS § 24 sätestab samuti üldised isikuandmete töötlemise nõuded, mida nii vastutav kui ka volitatud töötleja on

kohustatud järgima. Eelnõu § 33 punkt 1 on seotud isikuandmete töötlemise õigsuse põhimõttega, mille kohaselt isikuandmete töötleja on kohustatud tagama, et isikuandmed on õiged, ehk selle tagamiseks parandama ebaõiged isikuandmed. Punkt 2 on seotud isikuandmete töötlemise seaduslikkuse põhimõttega, mille kohaselt peaks vastutav või volitatud töötleja kustutama isikuandmed, kui isikuandmete töötlemine ei ole seaduse alusel lubatud. Samuti peaks isikuandmed kustutama, kui isikuandmete töötlemine rikub isikuandmete töötlemise põhimõtteid. Näiteks olukorras, kus isikuandmeid ei töödelda enam vastavalt algsele eesmärgile ning muul eesmärgil töötlemise alus puudub. Samuti olukorras, kus isikuandmeid on kogutud ülemääraselt ning nende töötlemine rikub isikuandmete kvaliteedi põhimõtet. Eelnõu § 33 punkt 3 sätestab, et vastutav või volitatud töötleja on kohustatud teavitama vastuvõtjat, kui isikuandmed on edastatud ebaseaduslikult või edastatud on ebaõigeid isikuandmeid. Nimetatud kohustus tagab isikuandmete töötlemise õigsuse põhimõtte rakendamise ning võimaldab vastuvõtjal ebaõiged isikuandmed parandada või kustutada. Selleks et tagada isikuandmete töötlemise nõuete järgimine ning andmekaitse kõrge tase, peab vastutav töötleja või volitatud töötleja tegema koostööd Andmekaitse Inspektsiooniga.

§ 34. Isikuandmete edastamise nõuded

Eelnõu §-s 34 on sätestatud konkreetsed nõuded, mida tuleb järgida isikuandmete edastamisel, mille eesmärk on tagada isikuandmete töötlemisel nende õigsus ning vähendada võimalusi, et isikuandmete edastamisel võivad isikuandmed muutuda ebaõigeks. Eelnõu § 34 lõikes 2 on sätestatud, et vastutav töötleja lisab võimaluse korral vajaliku teabe, mis võimaldab hinnata isikuandmete õigsust, täielikkust, usaldusväärsust ja ajakohasust. Selliseks teabeks on näiteks informatsioon selle kohta, millal isikuandmed on kogutud või kellelt isikuandmed pärinevad. See võimaldab isikuandmete vastuvõtjal hinnata, kuivõrd usaldusväärsed kõnealused isikuandmed on. Eelnõu § 34 lõike 3 kohaselt peab vastutav töötleja teavitama ka sellistest eritingimustest, mida kohaldatakse isikuandmete töötlemisele. Näiteks võib selliseks eritingimuseks olla teatud tehniline kaitsemeede, mida kohaldatakse kõnealuste isikuandmete töötlemisel, näiteks isikuandmete krüpteerimine või muud protseduurireeglid, mida isikuandmete töötlemisele kohaldatakse.

§ 35. Logimine

Eelnõu § 35 lõikest 1 tuleneb kohustus pidada logisid automatiseeritud viisil tehtavate teatud isikuandmete töötlemise toimingute kohta, mis on loetletud eelnõu § 35 lõike 1 punktides 1–7, ning lõikes 2 on täpsustatud, mida kõnealuste logide pidamisel peab olema võimalik tuvastada. Logide pidamise eesmärk on tagada isikuandmete töötlemisel töötlemistoimingute läbipaistvus ning võimaldada läbi viia nii sisemist kontrolli kui ka võimaldada Andmekaitse Inspektsioonil teostada tõhusalt järelevalvet isikuandmete töötlemise nõuete täitmise üle. Kuna ka logid on isikuandmed, tuleb säilitamise põhimõtte täitmiseks kehtestada logide säilitamise tähtajad ning need säilitamise tähtaja möödumisel jäädavalt kustutada. Logimise kohustus kohaldub kõikidele töötlemistoimingutele, mis teostatakse automatiseeritud viisil ehk infotehnoloogilise lahendise abil.

Eelnõu §-ga 35 pannakse nii vastutavale kui volitatud töötlejale kohustus tagada, et automatiseeritud töötlemisel toimub vähemalt teatud töötlemistoimingute logimine. Paragrahvi 35 lg 1 punktid 1-7 loetlevad töötlemistoiminguid, mille puhul on logimine

kohustuslik. Riigi Infosüsteemide Ameti poolt on logimine defineeritud kui „andmete käsitsi või automaatset salvestamist sellisel kujul, mis aitab leida vastuseid järgmistele küsimustele: mida keegi põhjustas (st kasutas), millal ta seda tegi ning milliseid vahendeid ta rakendas? Samuti peaks logimine aitama vastata küsimustele süsteemi seisundi kohta: kellel olid pääsuõigused, millised need olid ja millises ajavahemikus need kehtisid? IT-süsteemide usaldusväärse töö tagamiseks on vajalik, et infokoosluses saaksid logitud kõik turbe seisukohalt kriitilised sündmused. Logimise eesmärk on aidata mõista, miks ja kuidas leidsid IT-süsteemides ja rakendustes aset olulised muudatused, et hinnata süsteemide ja rakenduste turvet.“ (Allikas: ISKE kataloogides välja toodud selgitused logimise ja logide kohta on leitavad siin: https://www.ria.ee/public/ISKE/Logimine.pdf). Andmekaitse vaatevinklist on logimise eesmärk tagada, et automatiseeritud töötlemisel säilib jälg teostatud toimingu kohta, mis annab võimaluse kontrollida töötlemise õiguspärasust ning hinnata tehtud toimingute vastavust kehtestatud nõuetele.

Eestis kasutatakse logimist infosüsteemide puhul juba praegu, seega tegemist ei ole Eesti jaoks uudse kontseptsiooniga. Küll aga peavad vastutavad ja volitatud töötlejad, kes kasutavad töötlemisel infotehnoloogilisi lahendusi, tagama, et logimine hõlmab vähemalt § 35 lõikes 1 loetletud tegevusi. Samuti on oluline, et logid, mis kajastavad andmete lugemist, avalikustamist ja edastamist võimaldaksid kindlaks teha nende toimingute tegemise põhjenduse, kuupäeva ja kellaaja ning teabe isikuandmeid lugenud, avalikustanud või edastanud isiku kohta, samuti selliste isikuandmete vastuvõtjate nimed. Selline nõue on vajalik selleks, et näiteks isikuandmetega soetud rikkumise korral, kui on toimunud andmeleke, oleks võimalik tuvastada isikuid, kes on neid andmeid lugenud või teisele isikule edastanud. Õiguskaitseasutused peavad kontrollima, kas nende infosüsteemide logimisreeglid vastavad kõnealustele nõuetele ning vajadusel tegema täiendavaid infotehnoloogilisi arendusi

§ 36. Isikuandmete töötlemise toimingute registreerimine

Eelnõu §-s 35 sätestatu eesmärk on tagada, et isikuandmete töötlemisega seonduv teave oleks ülevaatlik ning kättesaadav eelkõige eesmärgil, et kontrollida isikuandmete töötlemise toimingute vastavust töötlemisega seonduvatele nõuetele. Tegemist on isikuandmete töötlemise toiminguid kajastava ülevaatliku teabega ning sätte eesmärk ei ole koostada iga isikuandmete töötlemise toimingu kohta eraldi dokumenti, mis sisaldab § 36 lõikes 1 või 2 nimetatud teavet. Isikuandmete registreerimise nõue tähendab, et vastutaval ja volitatud töötlejal peab olema ülevaade sellest, milliseid isikuandmeid ning millisel eesmärgil töödeldakse. Isikuandmete töötlemise toimingud võib registreerida kirjalikku taasesitamist võimaldavas vormis. Siinkohal on oluline, et nimetatud dokumendid oleks võimalik Andmekaitse Inspektsioonile vajaduse korral kättesaadavaks teha. Näiteks võib selleks olla ka isikuandmete töötlemise jaoks loodud eraldi programm, milles kajastub §-s 36 nimetatud teave, samuti võib selliseid dokumente pidada ka paberil.

Eelnõu § 36 reguleerib vastutava ja volitatud töötleja kohustust dokumenteerida tehtavate isikuandmete töötlemistoimingute liigid. Selline kohustus on vajalik selleks, et töötlejal oleks ülevaade tehtavatest toimingutest ja sellest, milliseid andmeid ja mis eesmärkidel töödeldakse. Ülevaate omamine on oluline element andmete töötlemise õiguspärasuse tagamiseks, võimaldades töötlejal kaardistada enda andmetöötlusprotsesse ning tehtavaid toiminguid. Näiteks peab õiguskaitseasutus dokumenteerima, et konkreetses asutuses töödeldakse vahistatud ja kinnipeetavate isikute identiteedi, tervise, karistuse, käitumise jms kohta. Samuti peab asutus määratlema, millistest allikatest andmeid kogutakse, millised on töötlemise eesmärgid (nt vahistuse või vangistuse täideviimine, tervishoiuteenuse osutamine

kinnipidamisasutuses, andmesubjekti ja teiste isikute turvalisuse tagamine jt. Samuti peab õiguskaitseasutus sätestama, kellele andmed edastatakse (nt politseile, tervishoiuteenuse pakkujale, kriminaalhooldajale jt). Eelnõu § 36 niisiis sätestab kohustuse dokumenteerida üldise raamistikuna, milliseid töötlemistoiminguid asutus teeb, mis isikuandmeid töödeldakse ja mis eesmärkidel.

§ 37. Andmekaitsealane mõjuhinnang

Andmekaitsealase mõjuhinnangu andmise kohustus teatud tingimustel tuleneb direktiivi artiklist 27 ning vastab oma sisult andmekaitsealase mõjuhinnangu läbiviimisele üldmääruse 2016/679 artikli 35 alusel. Andmekaitsealase mõjuhinnangu andmine on eelnõu § 35 lõike 1 kohaselt kohustuslik, kui isikuandmete töötlemise tulemusena ning töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes võib kaasneda suur oht füüsilise isiku õigustele ja vabadustele. Üldmääruse 2016/679 artikli 35 lõige 3 sätestab kindlad juhud, millal on andmekaitsealase mõjuhinnangu tegemine nõutav:
1) toimub isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb automatiseeritud töötlusel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt isikut;
2) määruse nr 2016/679 artikli 9 lõikes 1 sätestatud eriliiki isikuandmete või artiklis 10 sätestatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslik töötlemine;
3) avalike kohtade ulatuslik süstemaatiline jälgimine.

Seega võib järeldada, et nimetatud juhtudel võib kaasneda alati suur oht füüsilise isiku õigustele ja vabadustele. Samuti võib tõenäoliselt kaasneda suur oht juhul, kui võetakse kasutusele uusi tehnoloogiaid isikuandmete töötlemiseks. Erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhul, kui töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu, pseudonüümimise loata tühistamist või mõnda muud ulatuslikku majanduslikku või sotsiaalset kahju. Samuti juhul, kui andmesubjekt võib jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle. Suur oht võib tõenäoliselt kaasneda ka juhul, kui töödeldakse isikuandmeid, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi veendumusi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning süüteoasjades süüdimõistvate kohtuotsuste ja süütegude ning nendega seotud turvameetmete kohta või kui hinnatakse isiklikke aspekte, eelkõige töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega seotud aspektide analüüsimisel või prognoosimisel, et luua või kasutada isiklikke profiile. Samuti võib oht esineda olukorras, kus töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid. Suure ohu tõenäosus võib olla seotud ka isikuandmete töötlemisega ehk kui töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Mõjuhinnang peaks konkreetsemalt sisaldama kavandatavaid meetmeid, kaitsemeetmeid ja mehhanisme, et tagada isikuandmete kaitse ja tõendada vastavust isikuandmete töötlemise nõuetele. Mõjuhinnangud peaksid hõlmama isikuandmete töötlemise toimingu asjaomaseid süsteemi ja menetlusi, kuid mitte üksikjuhtumeid.

Teatud juhtudel võib olla mõistlik ja säästlik hõlmata andmekaitsealase mõjuhinnanguga rohkem kui üht projekti, näiteks juhul, kui avaliku sektori asutused või organid kavatsevad kasutusele võtta ühise rakenduse või töötlemisplatvormi või mitu vastutavat töötlejat kavatseb kasutusele võtta ühise rakenduse või töötlemiskeskkonna kogu tööstusharus või allharus või laialdaselt kasutatava horisontaalse tegevuse puhul. Eraldi mõjuhinnangu koostamine ei ole kohustuslik, kui eelnevalt on läbi viidud mõni andmetöötlemist ettevalmistav ametlik dokument, näiteks seaduse eelnõu seletuskiri või muu eelnõu ettevalmistav dokument.

Mõju hindamise kohustus ei laiene sellisele töötlemisele, sh infosüsteemidele, mida rakendatakse kuni direktiivi ülevõtmise tähtaja saabumiseni. Nimelt täpsustab direktiivi põhjenduspunkt 96, et liikmesriigid peavad viima andmetöötluse kooskõlla direktiivi sätetega, kuid seejuures tuleb arvestada, et selliste kohustuste täitmine, mis puudutab eelnevat konsulteerimist järelevalveasutusega, ei ole nõutav, kui andmetöötlus on õiguspärane ning kooskõlas kuni direktiivi jõustumiseni kehtinud õigusnormidega. Ühtlasi näeb üldmääruse 2016/679 art 35 lõige 10 ette, et juhul, kui mõjuanalüüsi sarnane analüüs on riigisisesest õigusest tulenevalt juba läbi viidud, ei pea mõjuanalüüsi uuesti tegema. Eeltoodust tulenevalt on justiitsministeerium seisukohal, et juba kasutuses olevatele infosüsteemide puhul ei ole eraldi mõjuhinnangut vaja ning sellisele tõlgendusele on viidanud ka Euroopa Komisjon.

§ 38. Eelnev konsulteerimine Andmekaitse Inspektsiooniga

Eelneva konsulteerimise kohustus tuleneb direktiivi artiklist 28 ning samasisuline kohustus on sätestatud ka üldmääruse 2016/679 artiklis 36. Kui andmekaitsealane mõjuhinnang näitab, et töötlemise tulemusena tekiks ohu leevendamise kaitsemeetmete ning turvameetmete ja -mehhanismide puudumise korral suur oht füüsilise isiku õigustele ja vabadustele, ning vastutav töötleja leiab, et seda ohtu ei ole võimalik kättesaadava tehnoloogia ja rakendamiskulude seisukohast mõistlike meetmetega leevendada, tuleks enne isikuandmete töötlemise toimingute alustamist konsulteerida järelevalveasutusega. Selline suur oht tekib tõenäoliselt isikuandmete teatud liiki töötluse ning töötlemisulatuse ja -sageduse tulemusena, mille tagajärjel võivad ka kahjustuda füüsilise isiku õigused ja vabadused või sekkutakse nendesse.

Eelnõu § 38 lõikest 6 tulenevalt võib Andmekaitse Inspektsioon koostada loetelu isikuandmete töötlemise toimingutest, mille puhul on eelnev konsulteerimine vajalik. See tähendab, et Andmekaitse Inspektsioonil on võimalik anda juhiseid selle kohta, millised on isikuandmete töötlemise toimingud, mille puhul eelnev konsulteerimine võiks olla vajalik.

§ 39. Andmekaitsespetsialisti määramine

Õiguskaitseasutusel on kohustus määrata andmekaitsespetsialist, kuid kohtud õigusemõistmise funktsiooni täites on sellisest kohustusest vabastatud. Direktiivi 2016/680 art 32 ja üldmääruse 2016/679 art 37 kasutavad inglise keeles sõnastust *data protection officer*. Eesti keelde on see termin tõlgitud kui „andmekaitseametnik“. Nimetatud tõlge tekitab vastuolu avaliku teenistuse seadusega (ATS), kus sätestatakse ametniku õiguslik seisund. Andmekaitsespetsialist ei pea olema ametnik ATSi tähenduses, mistõttu selguse huvides kasutatakse nimetust *andmekaitsespetsialist*.

Andmekaitsespetsialisti määramise kohustus tuleneb direktiivi 2016/680 artiklist 32. Vastav kohustus on kooskõlas ka määruse 2016/679 art 37 lõike 1 punktiga a, kuivõrd kõik õiguskaitseasutused on ka avaliku võimu kandjad. Seega on nii määruse 2016/679 kui ka kõnesoleva eelnõu 5. peatüki kohaldamisalasse jääva tegevuse puhul andmekaitsespetsialisti puudutav regulatsioon ühtne ning andmekaitsespetsialisti käsitlevad sätted ei erine eelnõu 5. peatükis sätestatust. Seetõttu võib üks andmekaitsespetsialist olla määratud nii määruse 2016/679 kui ka kõnesoleva eelnõu 5. peatüki kohaldamisalasse jääva isikuandmete töötlemise nõuete täitmise järele kontrollimiseks. Eesmärk on tagada andmekaitseametnikku puudutava regulatsiooni ühtsus ning samuti vähendada halduskoormust, mis kaasneks olukorras, kui isikuandmete töötlemise üldmääruse kohaldamisalasse ja direktiivi kohaldamisalasse jäävate isikuandmete töötlemise toimingute jaoks oleks ühe asutuse piires vaja määrata kaks erinevat andmekaitseametnikku. Lisaks on õiguskaitseasutusel võimalik eelnõu § 38 lõike 2 kohaselt määrata mitme asutuse või organi jaoks üks andmekaitsespetsialist olenevalt nende asutuste organisatsioonilisest struktuurist ja suurusest.

§ 40. Andmekaitsespetsialisti ülesanded

Eelnõu §-s 40 on sätestatud andmekaitsespetsialisti ülesanded, mida ta on kohustatud täitma kõnesoleva eelnõu 5. peatüki kohaldamisalasse jääva isikuandmete töötlemise toimingute puhul. Seega olukorras, kus on määratud üks andmekaitsespetsialist nii määruse 2016/679 kui ka kõnesoleva eelnõu 4. peatüki kohaldamisala jaoks, tulenevad andmekaitsespetsialisti ülesanded nii määruse 2016/679 artiklist 39 kui ka eelnõu §-st 40.

Eelnõu § 40 lõike 2 kohaselt ei täida kohtu andmekaitsespetsialist selle paragrahvi lõikes 1 nimetatud ülesandeid kohtu õigusemõistmisega seotud tegevuse suhtes. Kohtu õigusemõistmisega seotud tegevuse piiritlemisel tuleb lähtuda Eesti Vabariigi põhiseaduse §-s 146 sätestatud õigusemõistmise tähendusest. Tavapäraselt mõistetakse õigusemõistmise all vaidluste lahendamist ja kuriteo või väärteo toime pannud isikute süü kindlakstegemist ja nendele karistuste mõistmist. Õigusemõistmise sisu hõlmab põhiseadusega ja muude seadustega kohtule antud pädevuse.

Põhiseadus annab kohtule järgmise pädevuse, mida võib pidada õigusemõistmiseks:
1) seaduse ja muude õigustloovate aktide põhiseadusele vastavuse kontroll (§-d 15 ja 152);
2) avaliku võimu asutuse või ametiisiku sellise õigusakti või toimingu kontroll, mis rikub põhiseaduses sätestatud õigusi või vabadusi või on muul viisil põhiseadusega vastuolus (§ 15);
3) isikult vabaduse võtmise otsustamine (§-d 20 ja 21);
4) kuriteos süüdi tunnistamine (§ 22);
5) sundvõõrandamise seaduslikkuse üle otsustamine ning hüvitise suuruse määramine (§ 32);
6) loa andmine sekkumiseks sõnumite saladuse õigusesse (§ 43);
7) ühingu, liidu või erakonna tegevuse lõpetamine õigusrikkumise eest, samuti trahvi määramine nimetatud ühendustele (§ 48);
8) otsustamine, kas Riigikogu liige või Vabariigi President on kestvalt võimetu oma ülesandeid täitma (§-d 64 ja 68);

9) otsustamine, kas anda nõusolek Riigikogu esimehele Vabariigi Presidendi ülesannetes kuulutada välja Riigikogu erakorralised valimised või keelduda seadust välja kuulutamast (§ 83);
10) õiguskantsleri ja kohtuniku ametist tagandamine (§-d 140 ja 147).[17]

Eespool nimetatud tegevusi saab käsitada kohtu õigusemõistmise teostamiseks ning sellise tegevuse suhtes ei täida kohtu andmekaitsespetsialist oma ülesandeid.

Lisaks on kohtutele pandud ülesandeid, mis ei ole seotud õigusemõistmisega. Maakohtus asub kinnistusosakond, mis peab kinnistusraamatuid ja abieluvararegistrit; registriosakond, kus peetakse äriregistrit, mittetulundusühingute ja sihtasutuste registrit, kommertspandiregistrit ja laevakinnistusraamatut; kriminaalhooldusosakond, mis valvab kriminaalhooldusaluste käitumise ja neile kohtu pandud kohustuste täitmise järele. Kuna nimetatud tegevus ei ole käsitatav õigusemõistmisena, on andmekaitsespetsialist pädev täitma temale pandud ülesandeid.

§ 41. Andmekaitsespetsialisti ametiseisund

Andmekaitsespetsialisti ametiseisund vastab üldmääruse 2016/679 artiklis 38 sätestatule ning eelnõu 4. peatükis ei tehta andmekaitsespetsialisti ametiseisundi suhtes erisusi4. Seetõttu kohaldatakse õiguskaitseasutuse andmekaitsespetsialisti suhtes ka määruse 2016/679 artikli 38 lõigetes 3, 4, 5 ja 6 sätestatut.

§ 42. Isikuandmete töötlemise turvameetmed

Isikuandmete töötlemise turvameetmed on sätestatud kehtiva IKS §-s 25 ning on eelnõus säilinud põhiosas muutmata kujul. Lisandunud on andmetöötlussüsteeme puudutavad täiendavad nõuded. Nimelt on eelnõu § 42 punktis 9 sätestatud uus kohustus võtta turvameetmeid tagamaks, et andmetöötlussüsteeme oleks võimalik katkestuse korral taastada, ning punktis 10 on sätestatud kohustus tagada andmetöötlussüsteemi toimimine ja selles ilmnevatest toimimisvigadest teavitamine. Samuti on vastutav ja volitatud töötleja kohustatud võtma turvameetmeid eelnõu § 42 punkti 11 alusel, et ära hoida isikuandmete moonutamine süsteemirikete tagajärjel.

§ 43. Andmekaitse Inspektsiooni teavitamine isikuandmetega seotud rikkumisest

Direktiivi artiklist 30 tuleneb uus kohustus teavitada järelevalveasutust isikuandmetega seotud rikkumisest, mida kehtivas IKS-is ei ole kehtestatud. Selline kohustus on sätestatud ka määruse 2016/679 artiklis 33. Eelnõu § 43 lõike 1 kohaselt on teavitamine kohustuslik, kui rikkumine kujutab endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Nimelt võib isikuandmetega seotud rikkumine, kui seda asjakohaselt ja õigel ajal ei käsitleta, põhjustada füüsilistele isikutele füüsilist, varalist või mittevaralist kahju, nagu näiteks kontrolli kaotamine oma isikuandmete üle või õiguste piiramine, diskrimineerimine,

[17] Eesti Vabariigi põhiseadus, § 146. Kommenteeritud väljaanne, 2017.

identiteedivargus või pettus, rahaline kahju, pseudonüümimise loata lõpetamine, maine kahjustamine, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu või mõni muu ulatuslik majanduslik või sotsiaalne kahju asjaomasele füüsilisele isikule. Seetõttu, niipea kui vastutav töötleja saab teada, et toimunud on isikuandmetega seotud rikkumine, mis kujutab endast vastutava töötleja hinnangul ka tõenäoliselt ohtu füüsilise isiku õigustele ja vabadustele, peab ta eelnõu § 43 lõike 1 kohaselt viivitamata ja võimaluse korral 72 tunni jooksul pärast selle teada saamist teavitama rikkumisest Andmekaitse Inspektsiooni. Juhul kui volitatud töötleja saab teabe isikuandmetega seotud rikkumisest, on ta kohustatud sellest viivitamata teavitama vastutavat töötlejat, kes saab omakorda teavitada Andmekaitse Inspektsiooni. Eelnõu § 43 lõike 4 kohaselt peab inspektsiooni teavitamisest pärast 72 tunni möödumist esitama põhjenduse, miks ei olnud võimalik rikkumisest teavitada õigel ajal.

§ 44. Andmesubjekti teavitamine isikuandmetega seotud rikkumisest

Lisaks eelnõu §-s 43 sätestatud kohustusele teavitada Andmekaitse Inspektsiooni isikuandmetega seotud rikkumisest, on vastutav töötleja kohustatud viivitamata teavitama sellisest rikkumisest ka andmesubjekti. Kohustus teavitada andmesubjekti isikuandmetega seotud rikkumisest tuleneb ka üldmääruse 2016/679 artiklist 34.

Vastutav töötleja peaks ilma põhjendamatu viivituseta teavitama andmesubjekti isikuandmetega seotud rikkumisest, kui rikkumise tulemusena tekib tõenäoliselt suur oht füüsilise isiku õigustele ja vabadustele, et võimaldada andmesubjektil võtta vajalikke ettevaatusabinõusid. Teade tuleks saata andmesubjektile nii kiiresti kui mõistlikkuse piires võimalik ning tihedas koostöös järelevalveasutusega, pidades kinni tema või muude asjakohaste asutuste, nagu õiguskaitseasutuste suunistest. Näiteks kahju tekkimise otsese ohu leevendamise vajadus eeldaks andmesubjekti kohest teavitamist, samal ajal kui vajadus rakendada asjakohaseid meetmeid isikuandmetega seonduvate rikkumiste jätkumise või samalaadsete isikuandmetega seonduvate rikkumiste ärahoidmiseks võib õigustada hilisemat teavitamist. Erinevalt Andmekaitse Inspektsiooni teavitamisest võib andmesubjekti jätta teavitamata, kui on täidetud mõni eelnõu § 44 lõikes 3 sätestatud tingimustest. Eelnõu § 44 lõike 3 punkt 3 võimaldab jätta teavitamata konkreetse andmesubjekti, kui teavitamine tooks kaasa ebaproportsionaalsed kulud. Näiteks võib selline olukord esineda, kui isikuandmetega seotud rikkumisega on seotud suur hulk andmesubjekte. Sellisel juhul peab olema isikuandmetega seotud rikkumisest teavitatud siiski üldsust. Selline teavitamine võib toimuda näiteks teadaande esitamisega Ametlikes Teadaannetes või mõnes üleriigilises päevalehes.

Erinevalt määruse artiklist 34 on eelnõu § 44 lõikes 5 sätestatud alused, millal võib andmesubjekti teavitada hiljem, teavitada piiratud ulatuses või jätta ta teavitamata. Nimetatud alused on seotud valdkonna eripäraga ning andmesubjekti teavitamise piiramisel tuleb kaaluda andmesubjekti huve ja teiselt poolt eelnõu § 44 lõikes 5 sätestatud aluseid iga üksiku isikuandmetega seotud rikkumise puhul eraldi.

§ 45. Isikuandmete kolmandale riigile ja rahvusvahelisele organisatsioonile edastamise üldtingimused

Direktiivi 2016/680 artiklid 35–40 sätestavad piiriülese andmevahetuse reeglid. Kuivõrd EL on kõrge andmekaitsetasemega piirkond, rakendatakse isikuandmete edastamisel väljapoole EL-i eritingimusi, mille eesmärgiks on tagada isikuandmete kaitse ning andmesubjekti õiguste

tõhus rakendamine. Praegusel ajal on isikuandmete edastamine väljapoole EL-i reguleeritud näiteks IKS §-s 18, aga ka KrMS §-dega 489[3]–489[5] ning politsei ja piirivalve seaduse §-s 7[46]. Nimetatud sätted on direktiivi ülevõtmisel koondatud kõnesoleva eelnõu 4. peatükki.

Eelnõu §-s 45 on sätestatud isikuandmete edastamise üldtingimused, millest tuleb lähtuda iga kord isikuandmete edastamisel kolmandale riigile ja rahvusvahelisele organisatsioonile ning millega võetakse üle direktiivi 2016/680 artikkel 35. Eelnõu § 45 lõike 1 punktis 4 on sätestatud, et isikuandmete edastamine on lubatud, kui Euroopa Komisjon on vastu võtnud kaitse piisavuse otsuse või selle puudumisel on võetud eelnõu §-s 45 nimetatud kaitsemeetmed ning mõlema eelpool nimetatud aluse puudumisel on võimalik isikuandmeid edastada § 46 alusel eriolukorras. Samuti peavad isikuandmete edastamisel olema täidetud kõigi nende kolme aluse puhul muud eelnõu §-s 45 lõike 1 punktides 1, 2, 3 ja 5 sätestatud tingimused. Seega on üldreegli kohaselt vaja mitme tingimuse üheaegset esinemist, et edastada andmed kolmandale riigile või rahvusvahelisele organisatsioonile. Siiski on erandeid, mis andmeedastust lubavad. Nimelt on eelnõu § 45 lõike 2 kohaselt võimalik andmeid saatnud Euroopa Liidu liikmesriigi nõusolekuta edastada neid juhul, kui see on vajalik riigi või kolmanda riigi avalikku korda ähvardava vahetu ja tõsise ohu vältimiseks või riigi olulise huvi kaitseks. Eelnõu jätab siinkohal lahtiseks muu olulise huvi mõiste ning see sisustatakse vastavalt konkreetsest juhtumist. Näiteks saab oluliste huvide alla paigutada riigi kriitilise infrastruktuuri ja teenuste toimise, majandus- ja finantssüsteemi kaitse. Selle sättega kaetakse erandolukorrad, mille puhul on vaja kiiresti reageerida ja tegutseda ning ei ole võimalik hankida vajalikku nõusolekut. Seejuures tuleb aga arvestada, et sellisest andmevahetusest tuleb viivitamata informeerida andmed edastanud riiki. Ohu hindamine jääb seejuures andmeid töötleva ja andmeedastuse üle otsustava riigi (st kõnealusel juhul Eesti) ülesandeks.

2018. a veebruari seisuga on Euroopa Komisjon teinud piisava kaitse taseme otsused järgmiste riikide ja piirkondade suhtes: Andorra, Argentina, Fääri saared, Guernsay, Mani saar, Jersey, Uus-Meremaa, Austraalia, Šveits, Uruguay.

Ameerika Ühendriikidega on sõlmitud isikuandmekaitse raamleping, mis kehtestab üldreeglid isikuandmete vahetamisel EL-i ja USA õiguskaitseasutuste vahel. Raamleping ei anna siiski alust andmete edastamiseks, see peab tulenema konkreetse valdkonna lepingust (nt USA-ga sõlmitud lennureisijate broneeringuinfo vahetamise leping).

§ 46. Isikuandmete edastamine asjakohaste kaitsemeetmete kohaldamisel

Üldreeglina on isikuandmete edastamiseks vajalik Euroopa Komisjoni kaitse piisavuse otsus, kuid eelnõu § 46 kohaselt on andmete edastamine lubatud, kui kohaldatud on piisavaid kaitsemeetmeid, mis on sätestatud eelnõu § 46 punktides 1 ja 2. Sellised kaitsemeetmed võivad punkti 1 kohaselt sisalduda õiguslikult siduvas aktis, nagu näiteks kahepoolses rahvusvahelises lepingus või vastuvõtva riigi jõustunud õigusaktis, mida rakendatakse riikide õiguskorras ning mida võivad jõustada nende andmesubjektid, tagades andmekaitsenõuete täitmise ja andmesubjektide õiguste kaitse, mis hõlmab õigust tõhusale haldus- või õiguskaitsele. Euroopa Komisjon on selgitanud, et näiteks isikuandmete automatiseeritud

töötlemisel isiku kaitse konventsioon[18] ei ole selline õiguslikult siduv akt, mille alusel on isikuandmete edastamine punkti 1 alusel lubatud, sest sätestatud nõuded on liiga üldise tasemega ega sisalda kaitsemeetmeid, mida andmesubjektid võiksid tõhusalt jõustada. Siiski võib konventsiooni täitmise ja kohaldamise asjaolusid kõnealuses riigis arvesse võtta kaitsemeetmete hindamisel eelnõu § 46 punkti 2 alusel. Nimelt võimaldab eelnõu § 46 punkt 2 isikuandmete edastamist, kui vastutav töötleja on hinnanud kõiki edastamisega seotud asjaolusid ning leidnud, et võetud on kõik isikuandmete kaitse seisukohast vajalikud kaitsemeetmed. Andmete edastamist puudutavate kõigi asjaolude hindamiseks peaks vastutav töötleja võtma arvesse Europoli või Eurojusti ja kolmandate riikide vahel sõlmitud koostöökokkuleppeid, mis võimaldavad isikuandmete vahetamist. Vastutav töötleja peaks võtma arvesse ka asjaolu, et isikuandmete edastamisele kohaldatakse konfidentsiaalsuse kohustust ja sihtotstarbelisuse põhimõtet, millega tagatakse, et andmeid ei töödelda muul kui edastamisega seotud eesmärgil. Lisaks peaks vastutav töötleja võtma arvesse seda, et isikuandmeid ei kasutata selleks, et taotleda surmanuhtlust või muud julma ja ebainimlikku kohtlemist, anda selleks käsk või viia see täide. Kuigi kõnealuseid tingimusi võib lugeda asjakohasteks kaitsemeetmeteks, mis võimaldavad andmete edastamist, peaks vastutav töötleja saama nõuda täiendavaid kaitsemeetmeid.

Paragrahvi 46 lg 1 p 1 puhul võib vajadus tuleneda nii Eesti kui ka vastuvõtva riigi huvidest, nt saab kolmas riik pöörduda Eesti poole õigusabipalvega konkreetses kriminaalmenetluses ning nõuetekohase lepingu olemasolul on Eestil olemas alus isikuandmete edastamiseks taotlevale riigile, arvestades üldisi kriminaalõigusalase koostöö reegleid.

§ 47. Isikuandmete edastamine eriolukorras

Juhul kui Euroopa Komisjon ei ole võtnud vastu kaitse piisavuse otsust või puuduvad eelnõu §-s 46 sätestatud asjakohased kaitsemeetmed, on erandkorras isikuandmete edastamine lubatud eelnõu § 47 lõike 1 punktides 1–5 sätestatud vajaduse esinemisel. Eelnõu § 47 alusel võivad edastamistoimingud toimuda üksnes eriolukorras ning kõnealuseid erandeid tuleks tõlgendada kitsalt ning need ei tohiks võimaldada isikuandmete sagedast, ulatuslikku ja struktuurset edastamist ega andmete suuremahulist edastamist, vaid peaks piirduma rangelt vajalike andmetega. Samuti tuleb eelnõu § 47 lõike 2 kohaselt kaaluda andmesubjekti õigusi. Lõike 1 punktides 4 ja 5 sätestatud juhtudel ning olukorras, kus andmesubjekti õigused on kaalukamad, ei ole selline isikuandmete edastamine lubatud. § 47 lõike 1 punktide 3–5 puhul võib vajadus tuleneda nii Eesti kui ka vastuvõtva riigi huvidest, nt saab kolmas riik pöörduda Eesti poole õigusabipalvega konkreetses kriminaalmenetluses ning nõuetekohase lepingu olemasolul on Eestil olemas alus isikuandmete edastamiseks taotlevale riigile, arvestades üldisi kriminaalõigusalase koostöö reegleid. Samuti saab välisriigi politseiasutus pöörduda koostöötaotlusega Eesti politsei poole palvega edastada isikuandmeid. Vastavate õiguslike aluste olemasolul ja kooskõlas kehtivate koostööreeglitega on Eestil võimalik selliseid andmeid edastada.

§ 48. Isikuandmete edastamine kolmandas riigis asuvale vastuvõtjale

[18] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. https://www.riigiteataja.ee/akt/78300.

Üldjuhul edastatakse isikuandmeid pädevate õiguskaitseasutuste ja ametlike kanalite kaudu. Siiski võib konkreetsetel üksikjuhtudel juhtuda, et tavapärased menetlused, mis nõuavad ühenduse võtmist sellise kolmanda riigi asutusega, ei ole mõjusad või asjakohased, eelkõige seetõttu, et andmeid ei saaks edastada õigel ajal, või seetõttu, et kõnealune kolmanda riigi asutus ei austa õigusriigi põhimõtet või rahvusvahelisi inimõiguste norme ja standardeid, mistõttu liikmesriikide pädevad asutused võiksid otsustada edastada isikuandmed otse kõnealustes kolmandates riikides asuvatele vastuvõtjatele. Selline olukord võib tekkida siis, kui isikuandmeid on vaja edastada kiiresti, et päästa süüteo ohvriks langemise ohus oleva isiku elu või hoida ära lähiajal toimepandav kuritegu, näiteks terrorikuritegu. Andmete edastamise lubatavust ja põhjendatust peab hindama Eesti pädev asutus, kes soovib välisriigilt saadud andmeid edastada vahetult vastuvõtjale. Isikuandmete edastamine on lubatud sellises olukorras üksnes juhul, kui on täidetud kõik eelnõu § 48 punktides 1–5 sätestatud tingimused.

§ 49. Andmekaitse Inspektsiooni teavitamine ja isikuandmete edastamise dokumenteerimine

Direktiivi art 37 lõike 2 ning art 39 lõike 3 kohaselt peab edastav pädev asutus teatama isikuandmete edastamisest järelevalveasutusele. Direktiivis sätestatud nõue on üle võetud eelnõu § 48 lõikest 1, mille kohaselt peab vastutav töötleja andma ülevaate Andmekaitse Inspektsioonile kõnesoleva seaduse § 46 lõike punkti 2 ja § 48 alusel toimunud isikuandmete edastamisest vähemalt üks kord aastas. Sellisest ülevaatest peab selguma, millistel alustel on vastutav töötleja hinnanud eelnõu § 46 punkti 2 alusel kolmanda riigi või rahvusvahelise organisatsiooni tagatavaid kaitsemeetmeid. Nimetatud ülevaade ei pea sisaldama igal üksikul juhul isikuandmete edastamise põhjuseid, vaid võib olla esitatud kokkuvõtlikul kujul, mille alusel on järelevalveasutusel võimalik teostada järelevalvet isikuandmete edastamise seaduslikkuse üle.

Eelnõu § 49 lõige 2 võtab üle direktiivi art 37 lõikes 3, art 38 lõikes 3 ning art 39 lõikes 4 sätestatu. Nimelt kui isikuandmed edastatakse kõnesoleva seaduse § 46 punkti 2, § 47 lõike 1 või § 48 alusel, dokumenteerib vastutav töötleja sellise edastamise, sealhulgas edastamise kuupäeva ja kellaaja, vastuvõtva pädeva asutuse andmed, edastamise selgituse ja edastatud isikuandmed. Dokumentide pidamise eesmärk on tagada võimalus kontrollida, kas isikuandmete edastamine vastab kõnesolevas seaduses sätestatud nõuetele.

§ 50. Sõltumatu järelevalveasutuse moodustamine

Suur enamus Andmekaitse Inspektsiooni tegevusest, ennekõike see, mis puudutab tema ülesandeid, pädevust ja volitusi, on reguleeritud üldmääruse artiklites 51–59, mis on otsekohalduva iseloomuga, mille tõttu nende küsimuste reguleerimine uues seaduses ei ole asjakohane ega ka lubatud. Võrreldes kehtiva IKS-iga, mis nimetatud küsimusi reguleerib, ajakohastatakse sätteid, et ühtlustada üldist õiguslikku raami nimetatud küsimustes ennekõike nii avaliku teenistuse seaduse kui ka Vabariigi Valitsuse seaduse seisukohast.

Üldmääruse artikkel 51 ja õiguskaitseasutuste direktiivi art 41 näevad ette, et liikmesriigis peab isikuandmete töötlemisega seonduvate küsimuste õiguspärasuse üle järelevalvet teostama sõltumatu järelevalveasutus. Praegu kehtiva IKS-i kehtetuks tunnistamisega tunnistatakse kehtetuks ka 6. peatükk, mis reguleerib riiklikku ja haldusjärelevalvet, sealhulgas tervikuna Andmekaitse Inspektsiooni kui järelevalveasutuse tegevust.

Eelnõu paragrahvi 50 kohaselt on sõltumatu järelevalveasutus Andmekaitse Inspektsioon, kes on oma ülesannete täitmisel sõltumatu ja kes tegutseb, lähtudes uuest seadusest, üldmäärusest ning muudest seadustest ja nende alusel kehtestatud õigusaktidest.

§ 51. Andmekaitse Inspektsiooni juhi ametisse nimetamiseks nõutav kvalifikatsioon

Võrreldes kehtiva regulatsiooniga sätestatakse eelnõus nõutava kvalifikatsioonina see, et Andmekaitse Inspektsiooni juht peab olema juhtimiskogemusega kõrgharidusega isik, kellel on teadmised isikuandmete kaitse õiguslikust regulatsioonist ning info- ja kommunikatsioonitehnoloogiast, sealhulgas infosüsteemidest. Nimetatud säte täpsustab kehtivat regulatsiooni selles küsimuses, samas kaotab ära nõuded, mis on kehtestatud kehtiva IKS paragrahvi 34 lõigetes 2 ja 3. Kehtiv õigusraam katab nii avaliku teenistuse seaduse kui ka Vabariigi Valitsuse seaduse mõttes need küsimused.

§ 52. Andmekaitse Inspektsiooni juhi kandidaadi julgeolekukontroll

Vastavas sättes on säilitatud kehtiva IKS §-s 35 sisalduv regulatsioon Andmekaitse Inspektsiooni juhi kandidaadi julgeolekukontrolli kohta.

§ 53. Andmekaitse Inspektsiooni juhi ametisse nimetamine ja ametist vabastamine

Üldmääruse artikkel 54 näeb ette, et liikmesriik peab kehtestama järelevalveasutuse juhi maksimaalse ametiaja pikkuse, millega soovitakse kaasa aidata järelevalveasutuse sõltumatuse tagamisele. Sarnaselt teiste valitsusasutuste juhtidega (ATS § 23 lõige 2 punkt 3) kestab üks ametiaeg viis aastat. Enne ametisse nimetamist kuulatakse ära Riigikogu põhiseaduskomisjoni seisukoht.

§ 54. Andmekaitse Inspektsiooni pädevus sertifitseerimisasutuse akrediteerimisel

Üldmääruse art 43 lõige 1 ja art 55 näevad ette, et liikmesriik peab kehtestama asutuse, kes on pädev akrediteerima sertifitseerimisasutusi, millel on andmekaitse vallas asjakohased teadmised.

§ 55. Andmekaitse Inspektsiooni pädevus riikliku ja haldusjärelevalve teostamisel

Võrreldes kehtiva IKS-iga täiendatakse nimetatud küsimust ulatuses, mis on vajalik, et tagada kooskõla üldmääruses sätestatuga.

Eelnõu kõnesoleva paragrahvi lõikes 1 sätestatakse, et uues seaduses ja selle alusel kehtestatud õigusaktides, teistes seadustes direktiivi 2016/680 ülevõtmiseks kehtestatud nõuete täitmise üle, määruses nr 2016/679 sätestatud nõuete ning muudes seadustes isikuandmete töötlemisele kehtestatud nõuete täitmise üle teostab riiklikku ja haldusjärelevalvet Andmekaitse Inspektsioon. Nimetatud sättega täidab Eesti seadusandja

üldmääruse artiklist 57 tuleneva kohustuse, andes vastava pädevuse Andmekaitse Inspektsioonile.

Andmekaitse Inspektsioon teostab riiklikku ja haldusjärelevalvet kõnesolevas ja selle alusel kehtestatud õigusaktides ning muudes seadustes isikuandmete töötlemisele kehtestatud nõuete täitmise üle. Seega on Andmekaitse Inspektsioon pädev järelevalveasutus direktiivi 2016/680 artikli 41 mõttes. Lõikes 2 loetletakse Andmekaitse Inspektsiooni ülesanded, mis lisanduvad isikuandmete kaitse üldmääruses sätestatule.

Lõige 3 loetleb Andmekaitse Inspektsiooni volitused riikliku ja haldusjärelevalve teostamisel. Nimetatud lõige toetub õiguskaitseasutuste direktiivi artiklile 47.

§ 56. Riikliku järelevalve erimeetmed

Võrreldes kehtiva IKS paragrahviga 32^1 täiendatakse eelnõu kõnesolevat paragrahvi korrakaitseseaduse paragrahvidega 44, 52, 53. Vastavad paragrahvid viitavad järgnevatele meedetele: viibimiskeeld, vallasasja hoiulevõtmine ning hoiulevõetud vallasasja müümine või hävitamine.

Lisandunud meetmed on vajalikud, et vajadusel piirata isikute viibimist kohas, kus ei ole rakendatud piisavaid turvameetmeid, et tagada isikuandmete kaitse nõuete täitmine. Näiteks olukorras, kus kolmandate isikute viibimine võimaldab neil isikuandmeid töödelda, kuid neil puudub selleks õiguslik alus. Vallasasja hoiulevõtmine ning selle müümise ja hävitamise meede on vajalik näiteks isikuandmeid sisaldavate dokumentide hoiulevõtmisega, kui nende osas ei ole tagatud piisavad turvameetmed (näiteks prügikonteinerisse visatud patsientide andmed paberkandjal). Lisaks hoiulevõtmisele on võimalik vastavad dokumendid ka KorS § 53 alusel hävitada.

§ 57. Riikliku järelevalve erisused

Eelnõu nimetatud sättes kehtestatakse Andmekaitse Inspektsiooni õigus rakendada üldmääruse artiklis 58 sätestatud meetmeid riikliku järelevalve teostamiseks.

Lisaks säilitatakse lõikes 2 kehtiva IKS §-s 32^2 sätestatud riikliku järelevalve teostamise erisus, mis võimaldab Andmekaitse Inspektsioonil teha päringu elektroonilise side ettevõtjale üldkasutatava elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalike andmete kohta, välja arvatud sõnumi edastamise faktiga seotud andmed, kui muul viisil ei ole identifitseerimistunnustega seotud lõppkasutaja tuvastamine võimalik. Võrreldes varasemaga on sätet täiendatud lauseosaga, mis lubab teha päringu, kui muul viisil ei ole lõppkasutaja tuvastamine võimalik. Seda põhjusel, et üldkasutatava elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamine on küllaltki riivav meede. Selle sätte vajadus tuleneb direktiivist 2002/58, kus pealesunnitud teabe (rämpspost) korral meetmete võtmiseks tulenevad järelevalveasutuse volitused üldisest isikuandmete kaitse õigusest. Kuna rämpsposti saatja tuvastamine on praktiliselt võimalik ainult lõppkasutaja identifitseerimistunnuse kaudu, on vastava meetme säilitamine vajalik.

§ 58. Haldusjärelevalve erisused

Eelnõu paragrahvis 58 nähakse ette haldusjärelevalve erisused, mis seisnevad järgmises:
1) haldusjärelevalve teostamisel antud Andmekaitse Inspektsiooni ettekirjutuse täitmata jätmise korral võib Andmekaitse Inspektsioon pöörduda ettekirjutuse saanu kõrgemalseisva asutuse, isiku või kogu poole teenistusliku järelevalve korraldamiseks või ametniku suhtes distsiplinaarmenetluse algatamiseks;

2) teenistusliku järelevalve teostaja või distsiplinaarmenetluse algatamise õigust omav isik on kohustatud taotluse läbi vaatama selle saamisest alates ühe kuu jooksul ja esitama oma põhjendatud arvamuse Andmekaitse Inspektsioonile. Teenistusliku järelevalve või distsiplinaarmenetluse algatamise korral on järelevalve teostajal või distsiplinaarmenetluse algatamise õigust omaval isikul kohustus teavitada Andmekaitse Inspektsiooni viivitamata menetluse tulemustest;

3) Andmekaitse Inspektsioon pöördub ettekirjutuse täitmata jätmise korral protestiga halduskohtusse.

Ettekirjutuse all tuleb mõista üldmääruse artiklis 58 sätestatud korraldust.

§ 59. Sunniraha määr

Eelnõu paragrahviga 59 kehtestatakse sunniraha ülemmääraks kuni 20 000 000 eurot või ettevõtja puhul kuni 4 protsenti tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. Sunniraha ülemmäär on siis sama suur kui väärteokaristuse ülemmäär ning võimaldab Andmekaitse Inspektsioonil efektiivselt sekkuda isikuandmete töötlemise nõuete rikkumisel. Andmekaitse Inspektsioon peab sunniraha määramisel hindama, millises määras sunniraha rakendamine on Eesti kontekstis proportsionaalne.

§ 60. Kaebuse läbivaatamise tähtaeg

Eelnõu §-ga 60 kehtestatakse tähtaeg, mille jooksul peab Andmekaitse Inspektsioon lahendama kaebuse, mille on talle esitanud andmesubjekt. Tegemist on regulatsiooniga, mis on sarnane kehtiva IKS §-ga 38.

Lõikesse 3 on lisatud, et kaebuse läbivaatamise aeg pikeneb mõistliku aja võrra, mis on vajalik teiste järelevalveasutustega koostöö tegemiseks. Vastav säte käsitleb olukorda, kus Andmekaitse Inspektsioon on juhtiv järelevalveasutus isikuandmete kaitse üldmääruse art 56 lõike 3 mõttes ning viib läbi art 60 jj menetluse, kus ta kaasab teiste riikide järelevalveasutused. Kuna järelevalveasutuste kaasamine ning nende seisukohtade ootamine võtab aega, siis võib menetlusele kuluv aeg olla pikem, kui on käesoleva paragrahvi lõigetes 1 ja 2 ette nähtud 90 päeva.

§-d 61–70

Eelnõu 6. peatükis on sätestatud väärteokoosseisud, mis tulenevad üldmääruse artiklist 83 tulenevast kohustusest määrata trahvid üldmääruse 2016/679 sätete rikkumise eest. Eesti õigussüsteem ei võimalda määrata trahve (*administrative fines)* üldmääruse sätestatud üldkorra kohaselt, kuna haldustrahve Eesti õiguses ei eksisteeri. Sellest tulenevalt on võimalus üldmääruse art 83 lõikest 9 tulenevalt kohaldada trahve selliselt, et Eestis määrab trahvi järelevalveasutus (Andmekaitse Inspektsioon). Ka üldmääruse põhjenduspunktis 151 on selgelt välja toodud Eesti õigussüsteemi eripära, mille kohaselt ei võimalda Eesti õigussüsteem määrata trahve üldmääruses sätestatu kohaselt. Sellest tulenevalt on märgitud, et trahve käsitlevaid eeskirju saab kohaldada selliselt, et Eestis määrab trahvi järelevalveasutus väärteomenetluse raames, tingimusel et eeskirjade sellisel kohaldamisel nimetatud liikmesriikides on samaväärne toime nagu järelevalveasutuse määratud trahvidel. Rangete karistuste reguleerimine EL tasandil oli andmekaitsereformi üks olulisi eesmärke, kuivõrd seeläbi on võimalik kindlustada üldmäärusest tulenevate reeglite ühetaoline rakendamine EL-is. Sellest tulenevalt ei ole liimesriigil võimalik kalduda kõrvale üldmääruses sätestatud trahvide summadest. Küll aga on trahvide määramisel väga oluline tähelepanu pöörata rikkumisele, mille eest võib olla vajalik määrata trahv.

Kõnesoleva eelnõu 6. peatükk haakub karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) eelnõuga[19], mille justiitsministeerium on esitanud kooskõlastamiseks 18.08.2017. Nimetatud eelnõuga on kavandatud luua võimalus Euroopa Liidu õiguses sätestatud haldustrahvide kohaldamiseks väärteomenetluses ning ette näha teatud rikkumiste eest senisest oluliselt suurema rahatrahvi ülemmääraga väärteokaristusi.

Eelnõu 6. peatükis on sätestatud väärteokoosseisud tulenevalt üldmääruse artikli 83 lõike 4 punktidest a–c, lõike 5 punktidest a–e ja lõikest 6.

Oluline on märkida, et kehtiva IKS § 42 sätestab üsna üldise väärteokoosseisu isikuandmete töötlemise nõuete rikkumise eest. Kehtiva IKS § 42 lg 1 kohaselt on karistatav delikaatsete isikuandmete töötlemise registreerimiskohustuse, isikuandmete kaitse turvameetmete või isikuandmete töötlemise muude nõuete eiramine. Praktikas on kõnealust sätet rakendatud näiteks arsti poolt ebaseaduslikult e-tervise infosüsteemi kasutamisel ja muudel uudishimust tingitud juhtudel. Selline olukord säilib edaspidigi ning isikut, kes töötleb andmeid ebaseaduslikult, on võimalik vastutusele võtta. Uudishimust tingitud nõuete rikkumisele saab eeskätt rakendada eelnõu § 61 lõiget 1, mis viitab üldmääruse sätetele, sealhulgas artiklile 29 ja sellest tulenevate nõuete rikkumisele. Artikkel 29 kehtestab reeglid ja kohustused olukordadeks, kus isikuandmete töötlemine toimub vastutava või volitatud isiku nimel, näiteks lepingulises või tsiviilõiguslikus suhtes või teenistussuhtes. Seega on andmebaasile ebaseaduslik juurdepääs karistatav kui üldmääruse artiklist 29 tulenevate nõuete rikkumine. Ühtlasi on karistatav mistahes andmekaitse põhimõtte rikkumine, sealhulgas andmete töötlemine ilma õigusliku aluseta (§ 64).

Määruse nr 2016/679 artikli 83 lõike 2 kohaselt tuleb igal konkreetsel juhul trahvi määramise ja selle suuruse üle pöörata tähelepanu sama lõike punktides a–k nimetatud asjaoludele.

[19] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (väärteokaristuste reform, ELi õigusest tulenevad rahatrahvid) eelnõu: https://eelnoud.valitsus.ee/main/mount/docList/495deed0-3944-4bd9-b817-469ce0ad2845.

Näiteks rikkumise laadile, raskusele, kestusele, samuti mõjutatud andmesubjektide hulgale ja neile tekitatud kahju suurusele. Üldmääruse artikli 83 lõigetes 3 ja 4 sätestatud trahve kohaldatakse väärteomenetluses. See tähendab, et üldmääruse artikli 83 lõikes 2 nimetatud asjaolud on sellised, mis võimaldavad hinnata VTMS § 3^1 alusel, kas väärteomenetluse alustamine on toimepandud väärteo asjaolusid arvesse võttes põhjendatud, vajalik ja mõistlik. Sellest tulenevalt on üsna tõenäoline, et maksimummääras trahvide määramine oleks Eestis äärmiselt erandlik, sest järelevalveasutus (Andmekaitse Inspektsioon) peab igal juhul hindama, kas väärteomenetluse läbiviimine ning trahvi määramine on konkreetse rikkumise olemust ja iseloomu arvestades on vajalik ja proportsionaalne. Võib eeldada, et kõrgeimas määras trahvide määramine oleks Eestis ülimalt erandlik, arvestades Eestis tegutsevate ettevõtete majandustegevuse ulatust. Siiski ei saa seda täielikult välistada, näiteks juhul, kui Andmekaitse Inspektsioon oleks juhtiv järelevalveasutus piiriülese tegevusega ettevõtte korral ning ettevõtte üle-maailmne aastakäive on väga suur ning rikkumine väga raske. Igal juhul peab Andmekaitse Inspektsioon hindama erinevaid asjaolusid ning üldmäärus ei kirjuta ette, millises määras peab järelevalveasutus rakendama trahve teatud laadi rikkumiste korral, vaid tegemist on järelevalveasutuse kaalutlusõigusega. Seega peab järelevalveasutus tegema kahte erinevat kaalutlusotsust.

Esiteks, tuleb otsustada kas konkreetse rikkumise korral on väärteomenetluse alustamine vajalik ning proportsionaalne või on teiste järelevalvemeetmete rakendamine tõhusam. Teiseks, juhul kui järelevalveasutus otsustab alustada väärteomenetlust, tuleb erinevaid tegureid arvesse võttes otsustada määratava trahvi suurus. Artikkel 29 töögrupp on koostanud järelevalveasutuste jaoks suuniseid trahvide määramise kohta, mida leiab siit: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (nii inglise kui eesti keeles). Juhises on muuhulas rõhutatud, et nagu kõik parandusmeetmed üldiselt, peaksid trahvid piisavalt vastama rikkumise laadile, raskusele ja tagajärgedele ning järelevalveasutused peavad hindama kõiki juhtumi asjaolusid järjepideval ja objektiivselt põhjendatud viisil. Tõhususe, proportsionaalsuse ja heidutavuse hindamine peab iga juhtumi puhul kajastama ka valitud parandusmeetmega taotletavat eesmärki, milleks on kas uuesti tagada eeskirjade täitmine või karistada ebaseaduslikku käitumist (või mõlemad) (suuniste lk 6).

Kuivõrd Eestis rakendatakse üldmääruses ettenähtud haldustrahve väärteomenetluse raames, tuleb lähtuda väärteomenetluse üldreeglitest. VTMS § 3 lg 1 selgitab, et väärteomenetlusõigus kehtib füüsilise ja juriidilise isiku suhtes. Ainult kirjalikku hoiatamismenetlust (VTMS § 54^1) kohaldatakse ka riigi, kohaliku omavalitsuse ja avalik-õigusliku juriidilise isiku suhtes. Seega IKS-is ettenähtud väärteotrahve ei ole võimalik kohaldada riigi ja kohaliku omavalitsuse suhtes.

Rahatrahvide kohaldamise ühtse praktika tagamiseks on kohtuvälise menetleja juhil võimalik kasutada VTMS § 10 lg-s 2^1 sätestatud võimalust anda kõrgendatud ülemmääraga rahatrahvi kohaldamiseks üldiseid juhiseid.

Üldmääruse 2016/679 art 83 lõiked 4 ja 5 näevad ette, et trahv määratakse protsendina (vastavalt 2% või 4%) ettevõtja eelneva majandusaasta ülemaailmsest aastasest kogukäibest. Üldmääruses 2016/679 ei ole täpsustatud käibe arvutamiseks täiendavaid juhiseid. Sellest tulenevalt on mh juriidilise käibe kindlaksmääramisel asjakohane eelnimetatud karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu punkt 5, millega täiendatakse karistusseadustiku (KarS) üldosa §-ga 47^1 järgmiselt:

„§ 47[1]. Kõrgendatud ülemmääraga rahatrahv

(1) Põhjendatud juhul, eelkõige kui see on vajalik Eestile siduva rahvusvahelise kohustuse täitmiseks, võib käesolevas seadustikus või muus seaduses väärteo eest ette näha kõrgendatud ülemmääraga rahatrahvi. Sellisel juhul võib kohus või kohtuväline menetleja väärteo eest kohaldada rahatrahvi kuni:
1) 20 000 000 eurot või
2) kolmekordses väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas, kui sellist kasu või kahju on võimalik kindlaks teha.
(2) Juriidilisele isikule võib käesoleva paragrahvi lõikes 1 sätestatud juhul kohus või kohtuväline menetleja väärteo eest kohaldada rahatrahvi kuni:
1) 20 000 000 eurot;
2) kolmekordses väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas, kui sellist kasu või kahju on võimalik kindlaks teha, või
3) 15 protsenti juriidilise isiku käibest.

(3) Kui käesoleva seadustiku eriosas või muus seaduses ei sätestata teisiti, on käesoleva paragrahvi lõike 2 punktis 3 sätestatud käibeks juriidilise isiku käive väärteomenetluse alustamise aastale vahetult eelneval majandusaastal või kui isik on tegutsenud alla aasta, siis väärteomenetluse alustamise aastal.“

Väärteokoosseisud peegeldavad üldmääruse artikli 83 lõikeid 4 ja 5. Võrreldes kehtivate väärteokoosseisudega IKS-is ning KarS-is on ette nähtud senisest ulatuslikum väärteovastutus toimepandud andmekaitsealaste rikkumiste eest. Hetkel sätestab IKS § 42, et väärtegudeks on järgmised tegevused:

- delikaatsete isikuandmete töötlemise registreerimiskohustuse nõude rikkumine;
- isikuandmete kaitse turvameetmete nõuete eiramine või
- isikuandmete töötlemise muude nõuete eiramine.

Eriti IKS § 42 lg 1 sätestatud viimane süüteokoosseis (isikuandmete töötlemise muude nõuete eiramine) on oma olemusel väga lai ning sisuliselt hõlmab mistahes IKS-is sätestatud nõude rikkumist. Antud norm on väga lai ning seega ei ole võimalik ette näha, milliste tegude eest IKS § 42 tegelikkuses näeb ette väärteovastutuse. Muuhulgas on IKS § 42 kasutatud karistamiseks nn uudishimupäringute eest, st kui andmetele õiguspärast juurdepääsuõigust omavad füüsilised isikud on teostanud töötlemistoiminguid (nt andmete pärimine registritest) ilma õigusliku aluseta konkreetset toimingut teostada. Sellisel juhul on rikutud andmete töötlemise põhimõtteid ning töötlemine ei olnud õiguspärane. Seega paneb isik sellistel juhtudel toime väärteo, rikkudes isikuandmete kaitse seaduses sätestatud andmete töötlemise nõudeid. Nn uudishimupäringud on kahtlemata suur risk, eriti võttes arvesse Eesti infotehnoloogiliste lahenduste kasutamise ulatust. Uues IKS-is ei ole ette nähtud sama laia koosseisu, nagu seda on IKS § 42, kuid kõik samad elemendid oleksid jätkuvalt karistatavad. Nii sätestab uue IKS § 64 eraldi vastutuse isikuandmete töötlemise põhimõtete rikkumise eest (üldmääruse art 5 rikkumine), samuti loetleb § 62 erinevaid üldmääruses sätestatud nõudeid, mille rikkumise eest on ette nähtud väärteovastutus. IKS § 62 viitab muuhulgas üldmääruse artiklis 29 sätestatud nõuete rikkumisele. Üldmääruse art 29 sätestab, et kõiki üldmäärusest tulenevaid nõudeid peab täitma ka isik, kes töötleb isikuandmeid kas vastutava või volitatud töötleja nimel. Siia alla paigutuvad ka nn uudishimupäringud, mida teostavad füüsilised isikud, kes töötlevad isikuandmeid teise isiku nimel (näiteks ametnik on oma teenistusülesannetest lähtuvalt õigustatud teostama päringuid Rahvastikuregistrisse, perearst on õigustatud tegema oma patsiendi ravimeetodi otsustamiseks e-Tervise infosüsteemi jt).

Juhul, kui teise isiku nimel tehtava andmetöötluse korral rikutakse andmetöötluse põhimõtteid, nt tehakse päringuid ilma õigusliku aluseta, suuremas ulatuses kui vajalik jt, paneb isiku toime artiklis 29 sätestatud kohustuse rikkumise. Sellest tulenevalt saab isikut karistada väärteokorras IKS § 62 alusel.

§ 71. Isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute register

Kehtiva IKS § 31 alusel loodi delikaatsete isikuandmete töötlejate ja vastutavate isikute register. Kehtiva IKS-i kehtetuks tunnistamisest tulenevalt ei ole Andmekaitse Inspektsioonil õigust enam registrit pidada ning kehtivuse kaotab ka registri põhimäärus. Samas võib selles registris sisalduvaid andmeid olla vaja teatud aja jooksul töödelda. Seetõttu ongi sätestatud tähtaeg, millal on võimalik Andmekaitse Inspektsioonile teha päringuid registriandmetega tutvumiseks.

Nimetatud registri andmeid saab töödelda 5 aastat pärast käesoleva seaduse jõustumist. Viie aasta möödumisel registris olevad andmed kustutatakse. Andmekaitse Inspektsioonile on võimalik esitada taotlus registriandmetega tutvumiseks. Juurdepääsutaotluste lahendamisel lähtutakse AvTS-st.

§ 72. Seaduse kehtetuks tunnistamine

Isikuandmete kaitse seadus tunnistatakse kehtetuks. Kuna IKS-i hakkab asendama isikuandmete kaitse üldmäärus ning teatud osas kõnesolev seadus, siis tuleb kehtiv IKS kehtetuks tunnistada.

§ 73. Seaduse jõustumine

Kõnesolev seadus jõustub 2018. aasta 25. mail.

4. Eelnõu terminoloogia

Eelnõu terminoloogia toetub üldmääruse artiklis 4 sätestatud terminitele, mis on liikmesriikidele otsekohalduvad. Eelnõu 4. peatükis on õiguskaitseasutuste direktiivi ülevõtmisel paragrahviga 12 samuti üle võetud üldmääruse artiklis 4 sätestatu.

Direktiivi ülevõtmisest tulenevalt kasutatakse uute terminitena järgmisi:

Eelnõu paragrahvis 12 määratletakse *õiguskaitseasutus*.

Eelnõu 4. peatüki 5. jaos määratletakse termin *andmekaitsespetsialist,* mis vastab sisult üldmääruse 4. peatüki 4. jaos sätestatud terminile *andmekaitseametnik.*

5. Eelnõu vastavus Euroopa Liidu õigusele

Praegu reguleerib isikuandmete kaitse õigust üldseadusena IKS, millega on üle võetud direktiiv 95/46/EÜ. Alates 25. maist 2018 tunnistatakse direktiiv 95/46/EÜ kehtetuks, mida asendab otsekohalduv üldmäärus. Kuna kehtiva IKS-iga on üle võetud direktiiv, mis tunnistatakse kehtetuks, siis tuleb riigisiseselt tunnistada kehtetuks ka IKS. Alates 25. maist 2018 reguleerib isikuandmete kaitse õigust liikmesriigis otsekohalduv üldmäärus ning uus IKS, millega täpsustatakse ja täiendatakse üldmääruse küsimusi ulatuses, milles liikmesriikidele on see õigus antud.

Direktiiviga 2016/680 tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. Direktiivi 2016/680 ülevõtmise kohta on seletuskirjale lisatud võrdlustabel (lisa 1).

6. Seaduse mõjud

Vastavalt hea õigusloome ja normitehnika eeskirjale tuleb seletuskirjas anda ülevaade seaduse jõustumisega kaasnevatest mõjudest. Andmekaitsereformi kontekstis tuleneb aga suur osa muudatustest – ja seega ka mõjudest – Euroopa Parlamendi ja nõukogu otsekohalduvast määrusest. Määruse mõjusid on Euroopa Komisjon küll hinnanud, kuid seda menetluse suhteliselt varajases etapis[20]. Kuna eelnõust ja määrusest tulenevate mõjude üksteisest eristamine ei ole võimalik ega ka otstarbekas, siis on mõjuanalüüsis valitud lähenemine kirjeldada andmekaitsereformi mõjusid tervikuna, pöörates mõnevõrra suuremat rõhku muudatustele, mille osas jätab määrus liikmesriikidele otsustusruumi või mis on olemuselt suurema mõjuga. Arvestades muudatuste hulka, ei pruugi mõjuanalüüsis olla kajastatud ka väga vähese mõjuga muudatused.

6.1. Andmesubjekti õigusi ja isikuandmete töötlemise lubatavust puudutavad muudatused

Võrreldes praegu kehtiva IKS-iga sätestab üldmäärus oluliselt detailsemalt andmesubjekti õigused ning vastutava ja volitatud töötleja kohustused. Lisaks tuleneb määrusest täiendavaid kohustusi, mida kehtiv seadus ei reguleeri. Järgnevalt on antud ülevaade peamistest sisulistest muudatustest, mis puudutavad andmesubjekti õigusi ja isikuandmete töötlemise lubatavust:

a) Täpsustatakse isikuandmete töötlemise seaduslikkuse aluseid. Muu hulgas sätestatakse seadusliku alusena ka vastutava töötleja või kolmanda isiku õigustatud huvi, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused (art 6 lg 1 p f). Lisaks sätestab eelnõu ka isikuandmete töötlemise erialused: töötlemine ajakirjanduslikul eesmärgil, teadus-, ajaloouuringu või riikliku statistika vajadusteks, avalikes huvides toimuva arhiveerimise eesmärgil ning akadeemilise, kunstilise või kirjandusliku eneseväljenduse tarbeks. Nimetatud erialustest esimesed kaks on samasugusel kujul ka kehtivas seaduses.
b) Isikuandmete töötlemise põhimõttena sätestatakse piirang isikuandmete säilitamisele. Kuigi iseenesest ei ole tegemist uue piiranguga (kehtiva IKS § 24 kohaselt on isikuandmete töötleja kohustatud eesmärkide saavutamiseks mittevajalikud isikuandmed viivitamata kustutama või sulgema, kui seadus ei näe ette teisiti), siis suunab üldmäärus hindama andmete säilitamise vajadust juba töötlemise algusfaasis.

[20] Euroopa Komisjoni poolt koostatud esialgne mõjuanalüüs (ei sisalda hiljem EL-i nõukogu töörühmas tehtud muudatusi): http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf (25.10.2017)

Näiteks tuleb säilitamise ajavahemik või selle kriteeriumid määrata juba isikuandmete kogumise ajal (art 13 lg 2 p a), samuti isikuandmete töötlemise toimingute registreerimisel, kui see on võimalik (art 30). Selle kohustuse täitmine on senises praktikas olnud problemaatiline.

c) Reguleeritakse isikuandmete töötlemine muul eesmärgil kui see, milleks isikuandmed on kogutud. Artikli 6 lõige 4 sätestab tingimused, mida peab isikuandmete töötleja arvesse võtma, et teha kindlaks, kas edasine töötlemine on kooskõlas esialgse eesmärgiga. Kehtivas IKS-is ei ole edasine töötlemine selgelt reguleeritud.
d) Täiendatakse nõudeid teabele, mis andmetöötleja peab esitama andmesubjektile isikuandmete saamisel. Kehtiv seadus sätestab, et teave tuleb esitada andmesubjektilt nõusoleku küsimise ajal või enne seda (IKS § 12 lg-d 1 ja 3), üldmäärus, et isikuandmete saamise ajal (art 13 lg 1). Järgnevalt on toodud kehtiva ja uue regulatsiooni võrdlustabel.

Tabel 1. Nõudeid teabele, mis vastutav töötleja peab andma andmesubjektile isikuandmete saamisel

Kehtiv regulatsioon (IKS § 12)	Uus regulatsioon (artikkel 13)
• Isikuandmete töötleja või tema esindaja nimi, töötleja aadress ja kontaktandmed; • andmed, mille töötlemiseks luba antakse; • töötlemise eesmärk; • isikud, kellele andmete edastamine on lubatud; • kolmandatele isikutele edastamise tingimused; • andmesubjekti õigused edasise töötlemise osas; • delikaatsete isikuandmete puhul selgitus, et tegemist on delikaatsete isikuandmetega.	• Vastutava töötleja ning kui kohaldatav, siis vastutava töötleja esindaja nimi ja kontaktandmed; • asjakohasel juhul andmekaitseametniku kontaktandmed; • isikuandmete töötlemise eesmärk ja õiguslik alus; • kui isikuandmete töötlemine toimub töötleja õigustatud huvi alusel (art 6 lg 1 p f), siis teave vastutava töötleja või kolmanda isiku huvide kohta; • asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta; • asjakohasel juhul teave isikuandmete edastamise kohta kolmandale riigile või rahvusvahelisele organisatsioonile; • isikuandmete säilitamise ajavahemik või selle määramise kriteeriumid; • teave andmesubjekti õiguste kohta (õigus taotleda juurdepääsu oma isikuandmetele, õigus nõuda nende parandamist, kustutamist või töötlemise piiramist, õigus esitada vastuväide, õigus andmete ülekandmisele); • teave andmesubjekti õiguse kohta nõusolek igal ajal tagasi võtta (kui töötlemine toimub nõusoleku alusel); • teave õiguse kohta esitada kaebus järelevalveasutusele; • teave selle kohta, kas isikuandmete esitamine on õigusaktist või lepingust tulenev kohustus ning kas andmesubjekt on kohustatud isikuandmeid esitama; • teave automatiseeritud otsuste, sh profiilianalüüsi tegemise kohta.

Täienevad ka nõuded teabele, mis tuleb esitada juhul, kui andmed ei ole saadud andmesubjektilt (IKS § 15 *vs.* artikkel 14).

e) Kehtestatakse vanuseline alampiir, mille puhul on lapse nõusolek isikuandmete töötlemiseks infoühiskonna teenuste pakkumisel seaduslik (13 eluaastat). Kui laps on noorem kui 13-aastane, on töötlemine seaduslik üksnes sellisel juhul ja sellises ulatuses, milleks on nõusoleku andnud lapse seaduslik esindaja. Vastutav töötleja peab

tegema mõistlikud pingutused, et kontrollida, et nõusoleku on andnud lapse seaduslik esindaja.

f) Sätestatakse asjaolud, mille puhul on eriliiki isikuandmete (siiani *delikaatsete isikuandmete*) töötlemine lubatud (artikkel 9). Kehtivas IKS-is sellised tingimused puuduvad. Eelduslikult ei kaasne muudatusega praktikas märkimisväärset mõju.

g) Andmesubjekti nõusolek eriliiki isikuandmete töötlemiseks kehtib edaspidi 80 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti (hetkel on piiriks 30 aastat). Piiratakse ka isikute ringi, kellel on õigus pärast andmesubjekti surma anda luba andmesubjekti isikuandmete töötlemiseks. Praegu on see õigus andmesubjekti pärijal, abikaasal, alanejal või ülenejal sugulasel, õel või vennal, edaspidi üksnes andmesubjekti pärijal.

h) Säilib andmesubjekti õigus saada teavet enda isikuandmete töötlemise kohta. Uus regulatsioon täiendab loetelu teabest, mis tuleb vastutaval töötajal teatavaks teha:

Tabel 2. Andmesubjekti õigus tutvuda andmetega – nõuded teabele, mis vastutav töötleja peab esitama andmesubjektile andmesubjekti soovil

Kehtiv regulatsioon (IKS § 19 lg 1)	Uus regulatsioon (artikkel 15)
• Andmesubjekti kohta käivad isikuandmed; • isikuandmete töötlemise eesmärgid; • isikuandmete koosseis ja allikad; • kolmandad isikud või nende kategooriad, kellele isikuandmete edastamine on lubatud; • kolmandad isikud, kellele isikuandmed on edastatud; • isikuandmete töötleja või tema esindaja nimi ning isikuandmete töötleja aadress ja muud kontaktandmed.	• Töötlemise eesmärk; • asjaomaste isikuandmete liigid; • vastuvõtjad või vastuvõtjate kategooriad, kellele isikuandmed on avalikustatud või avalikustatakse, eelkõige kolmandates riikides olevad vastuvõtjad või rahvusvahelised organisatsioonid; • kavandatav isikuandmete säilitamise ajavahemik või selle määramise kriteeriumid; • teave õiguse kohta taotleda isikuandmete parandamist, kustutamist või piiramist või esitada vastuväide sellisele isikuandmete töötlemisele; • teave õiguse kohta esitada kaebus järelevalveasutusele (AKI-le); • teave automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta; • kui isikuandmed edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis teave kehtestatavatest kaitsemeetmetest.

i) Täiesti uue nõudena sätestatakse andmesubjekti õigus andmete ülekandmisele ühe vastutava töötleja juurest teise juurde. Ülekandmise õigus kohaldub, kui töötlemine põhineb andmesubjekti nõusolekul, lepingu täitmisel või kui andmeid töödeldakse automatiseeritult (vt täpsemalt artikkel 20). Kui see on tehniliselt teostatav, võib andmesubjekt nõuda, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale. Muudatuse tagajärjel suureneb erasektori andmetöötlejate halduskoormus,

seda eriti teatud valdkondades tegutsevate ettevõtjate jaoks (näiteks side- ja telekommunikatsioonieттevõtjad).

j) Sätestatakse selgelt andmesubjekti õigus esitada vastuväide teda puudutavate isikuandmete töötlemisele, mis toimub avalikes huvides oleva ülesande täitmiseks, avaliku võimu teostamiseks või vastutava töötleja või kolmanda isiku õigustatud huvi alusel. Kui vastuväide esitatakse otseturunduse eesmärgil toimuva töötlemise suhtes, siis ei tohi isikuandmeid sellisel eesmärgil enam töödelda.

Sihtrühm I – andmesubjektid
Sotsiaalne mõju

Andmekaitsereform puudutab suuremal või vähemal määral kõiki andmesubjekte ehk kõiki Eestis elavaid inimesi. 1. jaanuari 2017 seisuga on sihtrühma suuruseks seega 1 315 635 inimest. Andmekaitse üldmääruse ja direktiivi 2016/680 sihtrühmaks on Euroopa tasandil üle 510 miljoni inimese.[21]

Andmesubjektidele kaasneb muudatustega positiivne sotsiaalne mõju tõhusama isikuandmete kaitse kaudu. Suureneb informatsiooni hulk, mis andmesubjektile tuleb kättesaadavaks teha nii andmete saamisel kui ka hiljem andmesubjekti soovil, paraneb andmesubjekti võimalus kontrollida, kuidas ja kelle poolt tema isikuandmeid töödeldakse ja kellele edastatakse, ning esitada töötlemise suhtes vastuväiteid. Muudatused mõjutavad nii tooteid kui teenuseid, millega inimesed igapäevaselt kokku puutuvad. Näiteks on reformi tulemusel nutirakendustel keelatud küsida valimatult juurdepääsu kasutaja seadme funktsioonidele ja sisule, e-poe kaudu toote pakiautomaati tellides ei tohi aga küsida registreerumata kliendi aadressandmeid[22].

Täiesti uue õigusena sätestatakse õigus andmete ülekandmisele ühe töötleja juurest teise juurde, mis füüsiliste isikute jaoks võib lihtsustada näiteks teenusepakkuja vahetust (telekommunikatsiooniteenused, kommunaalteenused jm). Üldmääruses rõhutatakse korduvalt põhimõtet, et andmesubjekti tuleb informeerida selges ja lihtsas keeles – see puudutab näiteks töötlemiseks nõusoleku küsimist, teabe esitamist ning andmesubjekti teavitamist rikkumise toimumisest. Ei ole võimalik hinnata, kui palju on andmesubjektid seni oma õigusi seoses isikuandmete töötlemisega kasutanud ega kui palju hakatakse seda tegema pärast eelnõu ja üldmääruse jõustumist. Rolli mängivad siinkohal näiteks elanikkonna teadlikkus uuest regulatsioonist ning üldine usaldus avaliku ja erasektori vastu.

Uueks muudatuseks on ka alampiiri kehtestamine lapse vanusele, mille puhul on lapse nõusolek isikuandmete töötlemiseks infoühiskonna teenuste pakkumisel seaduslik. Eestis on kavas kehtestada alampiiriks 13 eluaastat[23]. Statistikaameti andmetel elas 1. jaanuari 2017 seisuga Eestis 188 677 alla 13-aastast last. Kuigi andmekaitsereformiga ei kaasne andmesubjektidele üldjuhul mingeid kohustusi ega täiendavat halduskoormust, siis edaspidi suureneb lapsevanemate vastutus lapse isikuandmete töötlemisel internetikeskkonnas (võib

[21] Elanikkonna andmed Eesti Statistikaameti ja Eurostati andmebaasidest.
[22] Need ja teised elulised näited andmekaitsereformiga kaasnevatest muudatustest on kättesaadavad Andmekaitse Inspektsiooni veebilehel: http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse (10.01.2018).
[23] Lapse nõusolekut isikuandmete töötlemiseks, sh liikmesriikide senist praktikat, on analüüsinud Macenaite ja Kosta (2017): http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096 (02.11.2017).

hõlmata kasutajaprofiili loomist, isikuandmete kogumist, otseturundust). Sõltuvalt teenusepakkujast võib see tähendada ka täiendavaid tegevusi vanemliku vastutuse tõendamiseks. Positiivne mõju seisneb lapse isikuandmete kuritarvitamise võimaluste vähenemises internetikeskkonnas, mis lisaks kuritegelikule tegevusele hõlmab ka sotsiaalseid probleeme (nt libakontod, veebikiusamine). Õiguslik regulatsioon ei saa loomulikult välistada praktikas olukordi, kui laps valetab enda vanuse kohta.

Väga vähese mõjuga on ka surnu isikuandmete töötlemist puudutavad muudatused (vt tabel 3). Võrreldes praegusega muutub andmete töötlemine mõnevõrra rangemaks, kuid mõju on sihtrühmadele (pärijad, andmetöötlejad) harv ja väikse ulatusega.

Tabel 3. Surnu isikuandmete töötlemist puudutavad muudatused

	Kehtiv regulatsioon	**Uus regulatsioon**
Periood pärast andmesubjekti surma, mille jooksul on töötlemine lubatud vaid nõusoleku või muul alusel	30 aastat	30 aastat
sh eriliiki andmete osas	30 aastat	80 aastat
Isikud, kes võivad anda nõusoleku	pärija, abikaasa, alaneja või üleneja sugulane, õde või vend	pärija

Andmesubjekti õigusi puudutavate muudatuste sihtrühm on suur (ligi 100% elanikkonnast) ning ka mõjude esinemise sagedus tõenäoliselt suur – isikuandmeid töödeldakse paljudes eri valdkondades nii avalikus kui erasektoris. Mõju ulatus on enamikul juhtudel pigem väike. Andmekaitsereformiga kaasnevat mõju andmesubjektidele võib tervikuna hinnata oluliseks HÕNTE § 46 tähenduses.

Sihtrühm II – isikuandmete töötlejad
Majanduslik mõju: ettevõtluskeskkond ja ettevõtete tegevus
Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Isikuandmete töötlejad võivad olla füüsilised või juriidilised isikud, avaliku sektori asutused või muud organid. Isikuandmeid töötleb enamik ettevõtjatest – kui mitte põhitegevuse raames, siis seoses tööõigusega või turunduslikel eesmärkidel – samuti valitsusasutused, kohalikud omavalitsused ja nende asutused, muud riigiasutused, avalik-õiguslikud juriidilised isikud ning kolmanda sektori vabaühendused.

Tabel 4. Valitsemissektori asutused ja ettevõtted põhitegevusalade lõikes 2016. aastal

EMTAK	**Tegevusala**	**Asutuste arv**	**%**
Valitsemissektor			
P85	Haridus	1223	39%
R91	Raamatukogude, arhiivide, muuseumide ja muude kultuuriasutuste tegevus	511	16%
O84	Avalik haldus ja riigikaitse, kohustuslik sotsiaalkindlustus	456	15%
R93	Sporditegevus ning lõbustus- ja vaba aja tegevused	325	10%

Q87	Hoolekandeasutuste tegevus	113	4%
Q88	Sotsiaalhoolekanne majutuseta	67	2%
D35	Elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine	63	2%
E36	Veekogumine, -töötlus ja -varustus	51	2%
Q86	Tervishoid	49	2%
L68	Kinnisvaraalane tegevus	47	2%
M71	Arhitekti- ja inseneritegevused	25	1%
M72	Teadus- ja arendustegevus	22	1%
R90	Loome-, kunsti- ja meelelahutustegevus	22	1%
M70	Peakontorite tegevus, juhtimisalane nõustamine	15	0%
H52	Laondus ja veondust abistavad tegevusalad	13	0%
E38	Jäätmekogumine, -töötlus ja -kõrvaldus, materjalide taaskasutusele võtmine	12	0%
	Muud tegevusalad	111	4%
Ettevõtted			
G	Hulgi- ja jaekaubandus, mootorsõidukite ja mootorrataste remont	21 625	18%
M	Kutse-, teadus- ja tehnikaalane tegevus	16 334	14%
A	Põllumajandus, metsamajandus ja kalapüük	12 041	10%
F	Ehitus	11 848	10%
C	Töötlev tööstus	8811	7%
H	Veondus ja laondus	8470	7%
L	Kinnisvaraalane tegevus	7446	6%
S	Muud teenindavad tegevused	7123	6%
J	Info ja side	6448	5%
N	Haldus- ja abitegevused	6054	5%
	Muud tegevusalad	14 250	12%

Statistikaameti andmetel oli 2016. aasta lõpus Eestis ligi 160 000 majanduslikult aktiivset majandusüksust. Võttes aluseks majandusüksuste institutsionaalsete sektorite klassifikaatori, siis valitsemissektorisse kuuluvaid asutusi ja avaliku sektori osalusega ettevõtteid oli nende hulgas 3125[24] (tabel 4). Majanduslikult aktiivseid ettevõtteid tegutseb Eestis üle 120 000 ning mittetulundusühinguid ja sihtasutusi ligi 32 000[25] – suurt osa neist mõjutavad andmekaitsereformiga kaasnevad muudatused.

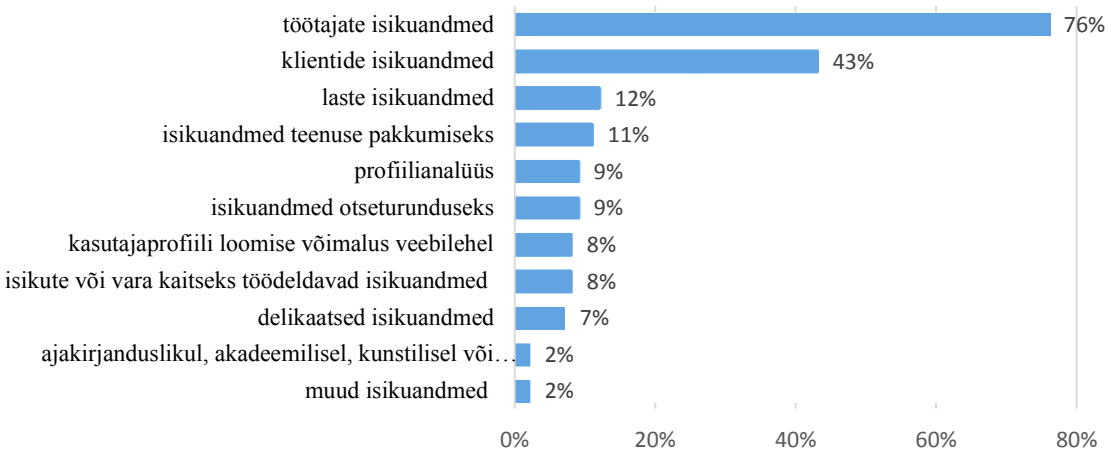
Justiitsministeeriumi poolt tellitud küsitlusuuringu[26] kohaselt töötleb isikuandmeid 85% Eestis tegutsevatest rohkem kui ühe töötajaga ettevõtetest. Siinkohal mängib olulist rolli ettevõtte suurus – rohkem kui 10 töötajaga ettevõtetest töötleb isikuandmeid 95%, samas kui mikroettevõtete hulgas on vastav näitaja 83% (ühe töötajaga või ilma töötajateta ettevõtete

[24] Arvestatud on valitsemissektori asutusi (klassifikaatorid S1311-S1314) ja avaliku sektori mittefinantsettevõtteid (S11001), arvestatud ei ole registrist kustutatud üksuseid. Andmed statistikaameti kodulehelt: http://www.stat.ee/majandusuksuste-klassifitseerimise-abiinfo (seisuga 09.11.2017).

[25] Andmed statistikaameti andmebaasist (majandus – majandusüksused) seisuga 09.11.2017.

[26] Turu-uuringute AS poolt teostatud ettevõtjatele suunatud küsitlus (seletuskirjas läbivalt kui küsitlusuuring) viidi läbi detsembris 2017. Uuringu valim koosnes 166 Eestis tegutsevast ettevõttest, kus töötas rohkem kui üks töötaja.

hulgas on näitaja tõenäoliselt mõnevõrra madalam). Enim töödeldakse töötajate ja klientide isikuandmeid, vastavalt 76% ja 43% kõigist uuringus osalenud ettevõtetest. Eelpool toodut arvesse võttes võib andmekaitsereformist mõjutatud sihtrühma hinnata suureks.



Joonis 1. Ettevõtete osakaal, kes koguvad või muul moel töötlevad vastavat liiki isikuandmeid
Allikas: Turu-uuringute AS

Andmesubjekti õigusi puudutavad muudatused on andmetöötlejatele eelkõige töökorraldusliku mõjuga (teabe esitamise kohustus, lapsevanema nõusoleku küsimine, edasise töötlemise lubatavus, andmete ülekandmine), kuid teatud juhtudel kaasneb ka otsene rahaline mõju. Kulud võivad kaasneda näiteks seoses infosüsteemide arendamisega, et tagada isikuandmete säilitamine vaid piiratud ajavahemikul, või andmete ülekandmiseks vajaliku funktsionaalsuse loomisega.

Puudub täpne ülevaade, kui paljusid riigi, kohaliku omavalitsuste või avalikke ülesandeid täitvate eraõiguslike isikute andmekogude infosüsteeme tuleb andmekaitsereformi valguses muuta ning millises ulatuses. Vajaduse üle otsustab andmekogu vastutav töötleja või infosüsteemi omanik. Riigi infosüsteemi haldussüsteemi RIHA kuulub eelnõu koostamise ajal 1405 infosüsteemi ja andmekogu. Tuginedes varasemale RIHA statistikale, siis umbes 64% infosüsteemidest on sellised, kus töödeldakse isikuandmeid, ning 31% sellised, kus töödeldakse delikaatseid isikuandmeid. Samas tuleb märkida, et isegi infosüsteemis, kus füüsiliste isikute kohta midagi ei kajastata, töödeldakse sellegipoolest näiteks administraatorite või sarnaste isikute andmeid (nt logides). Seega võib väita, et kõigis infosüsteemides töödeldakse ühel või teisel viisil isikuandmeid.[27]

Tabel 5. Infosüsteemide omanikud, kellel on enim RIHA-sse kuuluvaid infosüsteeme

Omanik	Infosüsteemide ja andmekogude arv
Politsei- ja Piirivalveamet	59
Maksu- ja Tolliamet	56

[27] Andmed Riigi Infosüsteemi Ametilt saadud RIHA statistika põhjal.

Sotsiaalministeerium	46
Registrite ja Infosüsteemide Keskus	39
Riigi Infosüsteemi Amet	38
Maaeluministeerium	34
Justiitsministeerium	33
Rahandusministeerium	30
Majandus- ja Kommunikatsiooniministeerium	28

Allikas: Riigi Infosüsteemi Amet

Kohalikud omavalitsused[28] on tundnud muret täiendava ressursivajaduse üle andmekaitsereformist tulenevate nõuete rakendamiseks, eelkõige mis puudutab infosüsteemide arendusvajadusi. KOV-ide kasutuses olevate andmekogud võib liigitada järgmiselt:

1. riiklikud andmekogud, mille volitatud töötlejad on KOV-id (nt ehitisregister, STAR, rahvastikuregister, EHIS, MAKIS jm);
2. infosüsteemid, mis on riigi poolt keskselt arendatud KOV-idele kasutamiseks (KOVTP, KOVMEN, VOLIS);
3. standardlahendused, mille kasutajad on KOV-id (nt dokumendihaldussüsteemid, HAUDI, ARNO, lemmikloomaregister jm);
4. KOV-ide enda poolt arendatud infosüsteemid.

Riiklike andmekogude arendamise eest vastutab ja kulud kannab andmekogu vastutav töötleja koostöös vastava ministeeriumi IT-asutusega. Riigi poolt keskselt KOV-idele kasutamiseks arendatud infosüsteeme on siiani arendanud ministeeriumid ning ka 2018. aastal vastutab nende arendamise eest Rahandusministeerium. Standardlahenduste puhul saavad tehtud arendused ja uuendused enda kasutusse kõik kasutajad. KOV-idele võib see tähendada mõningast (vähest) tõusu igakuises kasutustasus, kui standardlahenduse arendaja teeb kulusid selle vastavusse viimiseks uute andmekaitsenõuetega.

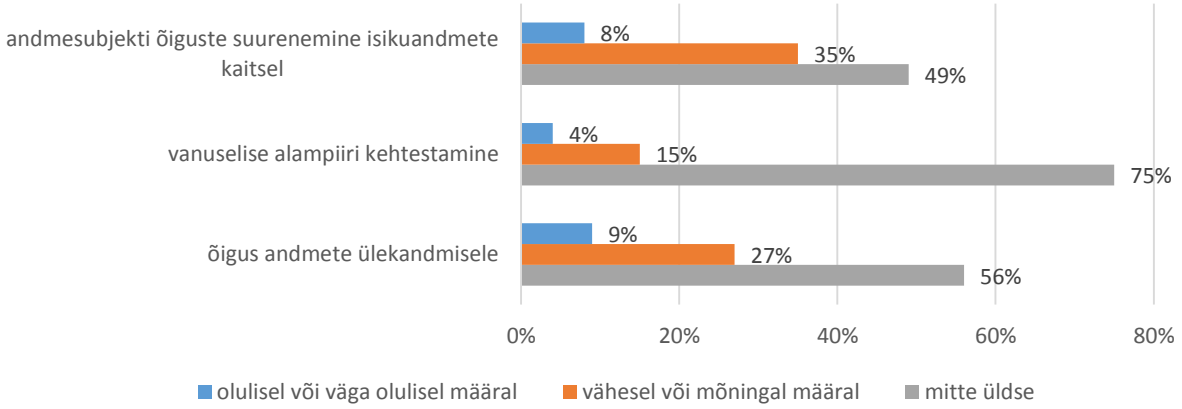
Seega tuleb KOV-idel kanda üksnes enda arendatud infosüsteemide arendamisega kaasnev kulu. RIHA-sse kuulub eelnõu koostamise ajal 377 infosüsteemi, mille omanik on kohalik omavalitsus (suure osa neist moodustavad standardlahendused). Enim infosüsteeme on Tallinna Linnakantseleil (24), Pärnu Linnavalitsusel (22), Tartu Linnavalitsusel (17) ja Jõhvi Vallavalitsusel (11).

AKI hinnangul on erasektori jaoks üheks kõige kulukamaks ja aeganõudvamaks rakendustegevuseks andmete ülekandmise õiguse võimaldamine. Artikli 20 lõige 1 sätestab, et andmesubjektil on õigus saada teda puudutavad isikuandmed struktureeritud ja üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele isikuandmete töötlejale, ilma et seda takistatakse. Lõige 2 täpsustab, et andmesubjektil on õigus nõuda, et vastutav töötleja edastab andmed otse teisele vastutavale töötlejale, kui see on tehniliselt teostatav. Seega kehtib andmete edastamisele tingimus, et see oleks tehniliselt teostatav, ning eelkõige on ettevõtjatel vaja tagada võimekus väljastada andmesubjektile tema isikuandmed struktureeritult, üldkasutatavas vormingus ja masinloetaval kujul. Erinevate

[28] Haldusreformi järgselt on Eestis 79 kohalikku omavalitsust.

andmetöötlejate infosüsteemide koosvõime tagamine võib teatud juhtudel olla väga ressursimahukas ning ettevõtjate huvi selle arendamiseks sõltub konkreetsest valdkonnast, seal tegutsevate ettevõtete suurusest ja arvust ning turu nõudlusest.

Teine muudatus, mille kohta on huvirühmad väljendanud seisukohta, et see toob kaasa ettevõtete halduskoormuse kasvu, on vanuselise alampiiri seadmine lapse nõusolekule isikuandmete töötlemiseks infoühiskonna teenuste kasutamisel. Küsitlusuuringu tulemused näitavad, et antud muudatus puudutab umbes viiendikku (19%) ettevõtjatest, seejuures 4% ettevõtjatest märgib, et muudatus mõjutab nende ettevõtte tegevust olulisel või väga olulisel määral.



Joonis 2. Ettevõtete hinnang kolme muudatuse mõju kohta ettevõtte tegevusele (küsimus: „*Palun hinnake, kas ja millisel määral mõjutavad muudatused teie ettevõtte tegevust*“)
Allikas: Turu-uuringute AS

Andmesubjekti õigusi puudutavate muudatuste mõju andmetöötlejatele on keskmise ulatusega – muudatustega kohanemine ei ole liigselt koormav ning ei piira andmetöötlejate põhitegevust ebaproportsionaalselt. Kohanemine uute nõuetega võib olla aja- ja ressursikulukam ettevalmistusperioodil, s.o enne üldmääruse jõustumist, vähenedes aja jooksul. Mõju esinemise sagedus varieerub andmetöötlejate lõikes ning sõltub näiteks sellest, kas andmeid töödeldakse põhitegevuse või toetavate tegevuste raames. Ebasoovitava riskina võib välja tuua ohu, et teatud erandjuhtudel võib andmetöötlejatele kaasneda ebaproportsionaalselt suur koormus võrreldes andmesubjekti õiguste kaitsest tuleneva kasuga (näiteks isikuandmete ülekandmine ühe vastutava töötleja juurest teise juurde, kui see on tehniliselt teostatav, kuid ressursimahukas).

Muudatustega kaasneb halduskoormuse kasv ettevõtjatele ning töökoormuse kasv avaliku sektori asutustele. Sihtrühma suurust arvestades võib muudatuste mõju tervikuna hinnata HÕNTE § 46 mõistes oluliseks.

6.2. Vastutava töötleja kohustusi puudutavad muudatused

Vastutava ja volitatud töötleja kohustused on suures osas sätestatud üldmääruse IV peatükis[29]. Muudatused on üldjoontes suunatud isikuandmete töötleja kohustuste ja vastutuse suurendamisele, et tagada isikuandmete turvaline ja läbipaistev töötlemine. See toob paratamatult kaasa halduskoormuse suurenemise ja täiendava ressursikulu. Kokkuvõte peamistest vastutava töötleja kohustusi puudutavatest muudatustest:

a) Võimaldatakse isikuandmete töötlemine kaasvastutavate töötlejate poolt, kes on ühiselt kindlaks määranud isikuandmete töötlemise eesmärgid ja vahendid (artikkel 26). Kaasvastutavad töötlejad peavad määrama vastutusvaldkonnad üldmääruse kohaste kohustuste täitmisel. Muudatusega kaasnev mõju on väike nii isikuandmete töötlejatele kui andmesubjektidele.
b) Kuigi tegemist ei ole uue muudatusega, siis rõhutab üldmäärus senisest enam vajadust rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid, mis on vajalikud andmekaitsepõhimõtete tõhusaks rakendamiseks ja kaitsemeetmete lõimimiseks isikuandmete töötlemisse (nt võimalikult väheste andmete kogumine, üksnes eesmärgipärane töötlemine). Rõhutatakse põhimõtet, et andmekaitse peab olema lõimitud isikuandmete töötlemisse ning rakenduma töötlemisele vaikimisi. Artiklis 32 tuuakse välja nimekiri võimalikest tehnilistest ja korralduslikest meetmetest, et tagada töötlemise turvalisus:
    - isikuandmete pseudonüümimine ja krüptimine;
    - võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;
    - võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral;
    - tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord.
c) Väljaspool Euroopa Liitu asuvale isikuandmete töötlejale, kes töötleb liidus asuvate andmesubjektide isikuandmeid, kehtestatakse kohustus määrata oma esindaja liidus (vt täpsemalt artikkel 27).
d) Oluliselt detailsemalt sätestatakse nõuded lepingule või õigusaktile, millega vastutav töötleja volitab isikuandmete töötlemise volitatud töötlejale (vt artikkel 28).
e) Isikuandmete töötlejal tuleb edaspidi registreerida tema vastutusel tehtavad isikuandmete töötlemise toimingud ning pidada sellekohast registrit (vt artikkel 30). Kohustust ei kohaldata vähem kui 250 töötajaga ettevõtjale või organisatsioonile, välja arvatud juhul, kui töötlemine kujutab tõenäoliselt ohtu andmesubjekti õigustele või vabadustele, töötlemine ei ole juhtumipõhine või töödeldakse eriliiki isikuandmeid või süüdimõistvate kohtuotsuste ja süütegudega seotud andmeid.
f) Kehtestatakse vastutava töötleja kohustus teavitada Andmekaitse Inspektsiooni isikuandmetega seotud rikkumisest. Teavitada tuleb põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul. Teavitama ei pea, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Teatud juhtudel on kohustus teavitada ka andmesubjekti.
g) Edaspidi tuleb enne kõrge riskiga isikuandmete töötlemise alustamist teha andmekaitsealane mõjuhinnang (artikkel 35). Mõjuhinnangu peavad tegema kõik need andmetöötlejad, kelle isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke

[29] Info olulisemate muudatuste kohta koos rakendamist puudutavate selgitustega on kättesaadav Andmekaitse Inspektsiooni veebilehel: http://www.aki.ee/et/andmekaitse-reform/andmetootleja-kohustused (02.11.2017).

arvesse võttes tekib tõenäoliselt suur oht füüsilistele isikute õigustele ja vabadustele. AKI hinnangul tehakse kõrge riskiga andmetöötlustoiminguid paljudes eri valdkondades[30], mistõttu on muudatusest mõjutatud isikute ring suur. Kui mõjuanalüüs kinnitab suure ohu riski, tuleb enne isikuandmete töötlemist konsulteerida Andmekaitse Inspektsiooniga (artikkel 36).

h) Isikuandmete töötleja on tulevikus kohustatud määrama andmekaitsespetsialisti, kui:
   - isikuandmeid töötleb avaliku sektori asutus või organ (avaliku võimu kandja);
   - töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud, mille laad, ulatus ja/või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise, või
   - töötleja põhitegevuse moodustab andmete eriliikide ulatuslik töötlemine või süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine.

   Muudatus mõjutab suurt hulka isikuandmete töötlejaid ning toob enamiku jaoks kaasa täiendava rahalise kulu seoses andmekaitsespetsialisti määramise, koolitamise või teenuse ostmisega. Andmekaitsespetsialist peab olema oma ülesannete täitmisel vaba ning alluma kõrgeimale juhtimistasandile, andmetöötleja peab tagama huvide konflikti vältimise.

i) Kaovad ära kohustused registreerida delikaatsete isikuandmete töötlemine ning määrata isikuandmete kaitse eest vastutav isik (IKS 5. ptk). Viimast hakkab sisuliselt asendama andmekaitsespetsialisti ametikoht.

j) Artikkel 40 sätestab võimaluse, et andmetöötlejaid esindavad ühendused võivad koostada toimimisjuhendeid, mis täpsustavad näiteks isikuandmete õiglast ja läbipaistvat töötlemist, isikuandmete kogumist, pseudonüümimist, teavitamist jm aspekte. Akrediteeritud asutus võib teostada järelevalvet, et toimimisjuhendi täitmise kohustuse võtnud andmetöötleja seda ka täidab.

k) Kehtestatakse regulatsioon andmekaitsealase sertifitseerimise võimaldamiseks. Sertifitseerimine on vastutavatele ja volitatud töötlejatele vabatahtlik, kuid aitab suurendada isikuandmete töötlemise läbipaistvust, tõendada üldmääruse nõuete järgimist ning annab signaali andmesubjektile, et tema isikuandmeid töödeldakse turvaliselt. Sertifikaadi saab väljastada sertifitseerimisasutus, mille on akrediteerinud Andmekaitse Inspektsioon.

l) Senisest detailsemalt sätestatakse tingimused, mille korral võib isikuandmeid edastada kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Võrreldes kehtiva regulatsiooniga (IKS § 18) suureneb mõnevõrra vastutava või volitatud töötleja vastutus veendumaks ja tõendamaks, et vastuvõtja töötleb isikuandmeid turvaliselt. Muudatuse mõju andmetöötlejatele on peamiselt töökorralduslik, andmete edastamist kolmandatele riikidele ei piirata senisest suuremas ulatuses, kuid tuleb selgemalt tõendada kaitse piisavus.

Sihtrühm I – isikuandmete töötlejad
Majanduslik mõju
Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, tuludele ja kuludele

[30] AKI koostatud loetelu valdkondadest, kus tehakse kõrge riskiga andmetöötlustoiminguid: http://www.aki.ee/et/andmekaitse-reform/mis-andmekaitsealane-mojuhinnang (02.11.2017)

Nagu punktis 6.1 selgitatud, on isikuandmete töötlejate sihtrühm tervikuna suur – Eestis on ligi 160 000 majanduslikult aktiivset majandusüksust, kellest enamikku mõjutavad isikuandmete töötleja kohustusi puudutavad muudatused.

Üldistatult jagunevad mõjutatud sihtrühmad järgmiselt:
1) valitsusasutused ja muud riigiasutused
2) kohalikud omavalitsused ja nende asutused
3) eraõiguslikud juriidilised isikud
4) avalik-õiguslikud juriidilised isikud
5) kolmanda sektori organisatsioonid.

Rahaline mõju on suurem neile, kellel tuleb edaspidi määrata andmekaitsespetsialist, koostada andmekaitsealaseid mõjuhinnanguid või registreerida tema vastutusel tehtavad isikuandmete töötlemise toimingud. Art 37 lg 1 sätestab, et andmekaitsespetsialisti peavad määrama kõik avaliku sektori asutused, välja arvatud õigust mõistvat funktsiooni täitvad kohtud. Valitsemissektorisse kuuluvaid üksusi ja asutusi ning avaliku sektori osalusega ettevõtteid on Eestis 3125, kuid lisaks neile laieneb andmekaitsespetsialisti määramise kohustus ka füüsilistele või eraõiguslikele juriidilistele isikutele, kes teostavad avalikku võimu või täidavad avalikke ülesandeid (nt halduslepingu alusel). Avaliku võimu kandjad võivad mitme asutuse või organi jaoks määrata ühe andmekaitsespetsialisti olenevalt nende organisatsioonilisest struktuurist või suurusest (art 37 lg 3). Selliseks näiteks võib olla kohaliku omavalitsuse juures asuv andmekaitsespetsialist, kes täidab andmekaitsespetsialisti ülesandeid ka kohalikule raamatukogule ja lasteaiale.

Kohalikud omavalitsused on üks andmekaitsereformist enim mõjutatud sihtrühmi. KOV-id töötlevad suures ulatuses oma elanike isikuandmeid, sh eriliiki isikuandmeid, mistõttu kohaldub neile enamik andmetöötleja kohustusi puudutavatest nõuetest: töötlemise toimingute registreerimine, andmekaitsealane mõjuhinnang, andmekaitsespetsialisti määramine, tehnilised ja korralduslikud meetmed turvalisuse tagamiseks jm. On tõenäoline, et vähemalt väiksemates KOV-ides hakkab andmekaitsespetsialist lisaks linna- või vallavalitsusele täitma ülesandeid ka teiste KOV-i asutuste juures. Esialgse prognoosi kohaselt võib andmekaitsespetsialisti määramisega seotud kulu KOV-ile jääda keskmiselt vahemikku 30 000–35 000 eurot aastas (sh palgakulu, majandus- ja koolituskulud)[31].

Erasektorile üldine andmekaitsespetsialisti määramise kohustus ei laiene. Küll aga tekib kohustus siis, kui töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud, mille laad, ulatus või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise. Andmekaitsespetsialisti kohustus kaasneb ka eriliiki andmete ulatusliku töötlemisega. Kuna tegemist ei ole üheselt defineeritud kriteeriumidega, siis peab selle üle otsustama iga andmetöötleja ise, lähtudes Andmekaitse Inspektsiooni ja Euroopa Komisjoni juhistest[32].

---

[31] Prognoos põhineb võrreldava tegevusala (audiitortegevus) keskmistel palgaandmetel ning koolituse maksumusel praeguse turupakkumise juures. Tegelik kulu sõltub KOV-i asukohast, suurusest ning andmekaitsespetsialisti määramise vormist.

[32] AKI suunised andmekaitsespetsialisti määramise kohta: http://www.aki.ee/et/andmekaitse-reform/kes-peavad-maarama-andmekaitsespetsialisti (09.11.2017)

Küsitlusuuringuga püüti välja selgitada, kui suurt hulka ettevõtetest võib andmekaitsespetsialisti määramine mõjutada. 12% ettevõtetest, kes isikuandmeid töötlevad, märkis, et nende ettevõtte põhitegevus sisaldab isikuandmete töötlemise toiminguid, mille laad, ulatus või eesmärk tingib andmesubjektide ulatusliku, korrapärase ja süstemaatilise jälgimise. 6% ettevõtetest töötleb ulatuslikult eriliiki isikuandmeid või süütegudega seotud isikuandmeid. Kahe tingimuse kokkuvõtmisel saab järeldada, et hinnanguliselt 14% ettevõtete andmetöötlus tingib andmekaitsespetsialisti määramise vajaduse. Tuleb rõhutada, et see osakaal võib olla alahinnatud, kuivõrd põhineb vaid ühe vastaja esialgsel hinnangul ning mitte ettevõtte andmetöötlustoimingute põhjalikul hindamisel[33].

Registriandmetele tuginedes saab üldistatult välja tuua äriühingud (tegevusalade kaupa), kellele võib rakenduda andmekaitsespetsialisti määramise kohustus, st nende põhitegevus võib hõlmata andmesubjektide ulatuslikku, korrapärast ja süstemaatilist jälgimist või eriliiki andmete või süütegudega seotud isikuandmete ulatuslikku töötlemist. Tegemist on informeeriva, kuid kindlasti mitte täpse ega ammendava loeteluga (tabel 6).

Tabel 6. Äriühingute arv, kelle põhitegevus võib hõlmata isikuandmete ulatuslikku, korrapärast ja süstemaatilist jälgimist[34]

Põhitegevusala	Arv	Hõlmatud EMTAK koodid
Kinnisvaraalane tegevus (sh kinnisvarabürood, kinnisvara haldus)	5043	6831, 68311, 6832, 68321, 68322, 68329
Finants- ja kindlustustegevus (sh investeerimine, laenuandmine, pangad, finantsnõustamine, kindlustus, fondide valitsemine jm)	3822	64191, 64301, 6492, 64921, 64929, 65111, 65121, 65301, 66111, 6612, 66121, 66129, 6619, 66191, 66199, 66211, 66221, 66291, 66301
Jaemüük posti või interneti teel	3182	47911
Haldus- ja abitegevused (sh tööhõiveagentuurid, reisibürood, turvatöö, inkassoteenused jm)	2655	78101, 78201, 78301, 79111, 79121, 80101, 80201, 80301, 82911
Tervishoid ja sotsiaalhoolekanne (sh üldarstiabi, hambaravi, õendusabi jm)	2412	86101, 8621, 86211, 86231, 8690, 86901, 86902, 86903, 86904, 86905, 86906, 86909, 87101, 8720, 87201, 87301, 879, 8790, 87901, 87909
Info ja side (sh andmetöötlus, veebihosting, veebiportaalid, telekommunikatsioon, ajakirjade kirjastamine jm)	2407	58121, 58131, 58141, 6110, 61101, 61109, 6120, 61201, 61209, 61301, 61901, 63111, 63121
Kutse-, teadus- ja tehnikaalane tegevus (sh teadus ja arendus biotehnoloogia vallas, reklaami vahendamine, turu-uuringud ja küsitlused)	1126	72111, 7312, 73121, 73201

[33] Küsitlusuuring sisaldas muu hulgas ka küsimust selle kohta, kas ettevõte plaanib määrata andmekaitsespetsialisti. Selgus, et vaid 8% ettevõtjatest plaanib seda teha (18% ei osanud öelda). Tulemused viitavad asjaolule, et andmekaitsespetsialisti määramise kohustust võidakse alahinnata.

[34] Äriregistri andmed majanduslikult aktiivsete äriühingute kohta (st andmed ei sisalda MTÜ-sid, SA-id ja riigi- ja kohaliku omavalitsuse asutuste riiklikusse registrisse kuuluvaid asutusi, 02.02.2017).

Majutus (sh hotellid, motellid, külalistemajad)	584	5510, 55101, 55102, 55103

Allikas: äriregister

Vastavalt üldmääruse artikli 37 lõikele 6 võib andmekaitsespetsialist olla andmetöötleja koosseisuline töötaja või täita ülesandeid teenuslepingu alusel. Üks andmekaitsespetsialist võib töötada mitme andmetöötleja heaks, samuti võib kontsern määrata ühise andmekaitsespetsialisti, tingimusel et ta on hõlpsasti kättesaadav kõikidest tegevuskohtadest. Huvirühmadega konsulteerimisel on avaldatud arvamust, et andmekaitsespetsialist peab ettevõtet ja selle tööprotsesse väga hästi tundma, mistõttu võiks tegemist olla pigem ettevõttesisese töötajaga. AKI hinnangul vastab andmekaitsespetsialisti ametikohale tänases Eesti seaduses ettenähtud isikuandmete töötlemise eest vastutav isik, keda on seni määratud üle 1100[35]. Tuleb märkida, et andmekaitsespetsialisti määramise kohustus ei ole Euroopa mõistes uus regulatsioon – näiteks Saksamaal töötab juba praegu hinnanguliselt 90% ettevõtete juures andmekaitseametnik[36].

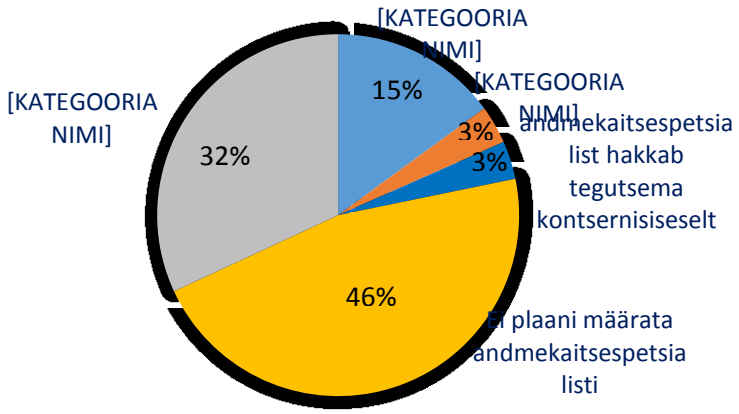
Lähtudes andmekaitsespetsialisti ülesannetest ja kompetentsidest, on huvirühmade hinnangul uue ametikohaga võrreldavaks tegevusalaks auditeerimine. Ühe suurema töövahendusportaali andmetel on audiitori keskmine netokuupalk 1559 eurot[37] (palgakulu tööandjale 2642 eurot kuus ja 31 704 eurot aastas). Kulud kaasnevad ka andmekaitsespetsialisti koolitamisega – kõrgkoolide juures pakutavate andmekaitsespetsialisti täiendkoolituste hind jääb eelnõu koostamise ajal vahemikku 1400–2400 eurot, muude koolitajate poolt pakutavate lühikoolitused hind aga ligikaudu paarsaja euro kanti. Milliseks kujuneb andmekaitsespetsialisti teenuse hind, selgub tõenäoliselt turukonkurentsi olukorras.

Vähemalt ettevõtjate puhul viitavad andmed sellele, et andmekaitsespetsialistina nähakse eelkõige olemasolevat koosseisulist töötajat ning uue ametikoha loomist ei planeerita (joonis 3).

[35] Andmekaitse Inspektsiooni peadirektori ülevaade, lk 10: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf .

[36] Lisaks Sksamaale on andmekaitsespetsialisti regulatsioon olemas ka Prantsusmaal ja Rootsis. Rahvusvaheline privaatsusvaldkonna spetsialistide ühendus (IAPP) on hinnanud, et üldmääruse kohaldumisest tulenevalt tekib maailmas vajadus umbes 75 000 uue andmekaitsespetsialisti järele. Tegemist on konservatiivse hinnanguga, mis jättis vaatluse alt välja kõik Euroopa väikese ja keskmise suurusega ettevõtted https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/ (11.01.2018)

[37] Palgaandmed ametikohtade järgi: http://www.palgad.ee/salaryinfo. Tegemist on valimi põhjal saadud tulemusega, mis ei pruugi olla üldistatav üldkogumile.



Joonis 3. Andmekaitsespetsialisti määramise vorm ettevõtete hulgas, kes töötlevad isikuandmeid (vastused küsimusele: „*Millises vormis plaanite andmekaitsespetsialisti määrata*?“)
Allikas: Turu-uuringute AS

Täiesti uuteks kohustusteks andmetöötlejatele on ka isikuandmete töötlemise toimingute registreerimine (artikkel 30) ja andmekaitsealase mõjuhinnangu koostamine (artikkel 35). Registreerimise kohustus tekib enam kui 250 töötajaga ettevõtjatele, samuti ettevõtjatele, kelle teostatav töötlemine kujutab tõenäoliselt ohtu andmesubjekti õigustele ja vabadustele, töötlemine ei ole juhtumipõhine või töödeldakse eriliiki isikuandmeid või süütegudega seotud andmeid. Kuigi üle 250 töötajaga ettevõtted moodustavad Eestis kõigest 0,2% ettevõtetest[38], siis teistest tingimustest tulenevalt puudutab nõue tõenäoliselt suuremat hulka andmetöötlejaid (näiteks süstemaatilise andmete töötlemise puhul). Mõjuhinnangu peavad tegema kõik need andmetöötlejad, kelle isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsilistele isikute õigustele ja vabadustele suur oht. Üldmäärus täpsustab juhte, millal mõjuhinnangu tegemine on nõutav ning muu hulgas sätestab järelevalveasutuse (AKI) kohustuse koostada ja avalikustada loetelu andmetöötluse toimingutest, mille suhtes nõuet kohaldatakse.

Turvalise töötlemise põhimõte ei tohiks Eesti andmetöötlejatele olla uus põhimõte – kehtiv IKS sätestab, et isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitama töötlemise, avalikuks tuleku või hävimise eest (IKS § 6 p 6). Turvalisuse põhimõte sisaldub ka üldmääruses (artikkel 5 lg 1 p f).

Kehtivas seaduses sätestatud ja üldmääruses loetletud turvameetmete vahel ei ole samuti olulisi erinevusi[39]. Uuenduslikuks on pseudonüümimise ja krüptimise kui konkreetsete meetmete nimetamine ning meetmete tõhususe korrapärase testimise nõue. Üldmäärus rõhutab senisest enam turvameetmete proportsionaalsust – tehniliste ja korralduslike meetmete rakendamisel tuleb arvesse võtta teaduse ja tehnoloogia viimast arengut, rakendamise kulusid, töötlemise laadi, ulatust, konteksti ja eesmärke ning võimalikke ohtusid füüsiliste isikute õigustele. Märgime, et kuigi artikkel 32 nimetab konkreetselt pseudonüümimist, siis võivad sobivateks kaitsemeetmeteks olla ka muud meetodid, mis tagavad andmete isikustamata töötlemise (nt anonüümimine). Anonüümsetele andmetele ei

[38] Statistikaameti andmetel tegutses Eestis 2016. aastal 196 ettevõtet, kus oli 250 või rohkem töötajat.
[39] IKS-i 4. peatükk *vs.* üldmääruse artikkel 32.

tuleks kohaldada andmekaitse põhimõtteid[40]. Turvameetmete rakendamisel võivad andmetöötlejatel tekkida kulud pigem põhjusel, et ka praegu ei ole täidetud kõik turvalise andmetöötluse nõuded (nt andmetele juurdepääs ei ole piiratud üksnes isikutele, kellele on töötlemine lubatud; puudub ülevaade isikuandmete edastamise kohta jm).

Eelnõu koostaja hinnangul avaldavad isikuandmete töötleja kohustusi puudutavad muudatused sihtrühmale ulatuslikku ja sagedast mõju, paljudel juhtudel läbi otsese rahalise kulu. Kogukulude hindamine nii era- kui avalikule sektorile eeldaks mitmete eelduste püstitamist ning ka siis oleks hinnang väga ligikaudne – mitmete nõuete kohaldamise ja selle ulatuse üle otsustab andmetöötleja ise tulenevalt enda andmetöötluse eripärast. Küsitlusuuringus paluti ettevõtjatel endal hinnata andmekaitsereformist tulenevat ligikaudset kogukulu ettevõttele. Kuna rahalise hinnangu andis vaid väike osa valimist (14%), siis ei saa tulemusi laiendada üldkogumile, kuid märgime, et hinnangud jäid vahemikku 0–70 000 eurot.

Eeltoodut arvesse võttes hindame muudatuste mõju sihtrühmale HÕNTE § 46 mõistes oluliseks. Muudatuste tulemusel suureneb nii avaliku, era- kui ka kolmanda sektori halduskoormus. Elanike halduskoormus ei muutu.

Sihtrühmad II – tulevased andmekaitseametnikud, teenust osutama hakkavad ettevõtted, ülikoolid ja teised koolitajad, sertifitseerimisasutused, andmesubjektid
Majanduslik mõju: ettevõtluskeskkond ja ettevõtete tegevus
Sotsiaalne mõju: tööturg

Andmekaitsespetsialisti regulatsiooniga tekib tööturul vajadus uue, praegu puuduva ametikoha järele, mis eeldab ka vastava kvalifikatsiooniga töötajate olemasolu. Turul on tekkinud nii nõudlus kui pakkumine erinevate andmekaitsega seotud koolituste, sh ka andmekaitsespetsialisti koolituste järele. Teenuseid pakuvad näiteks ülikoolid, advokaadibürood ning koolitus- ja konsultatsioonifirmad. Esimesed teenusepakkujad on hakanud pakkuma ka andmekaitseteenuseid, et aidata klientidel üldmääruse jõustumise ajaks enda andmetöötlemine nõuetega kooskõlla viia. Paraku ei ole võimalik täpselt hinnata, kui paljusid ettevõtteid regulatsioon otseselt või kaudselt puudutama hakkab või milline saab olema mõju turuosalistele ja tööjõuturule.

Tõendamaks, et andmetöötleja isikuandmete töötlemise toimingud vastavad üldmäärusele, võib akrediteeritud sertifitseerimisasutus, Andmekaitse Inspektsioon või andmekaitsenõukogu väljastada andmetöötlejale sellekohase sertifikaadi. Sertifitseerimine on andmetöötlejatele vabatahtlik, küll aga on liikmesriik kohustatud välja töötama sertifitseerimisasutuste akrediteerimisprotsessi ning julgustama sertifitseerimismehhanismide ja andmekaitsepitserite ja –märgiste kasutuselevõttu. Võimalikeks sertifitseerimisasutusteks võivad tulevikus olla erialaliidud, mis oskaksid arvestada valdkonna ettevõtete andmetöötluse vajaduste ja eripäradega. Riigiportaali www.eesti.ee andmetel tegutseb Eestis 55 erialaliitu[41]. Sertifitseerimisasutustele antakse akrediteering maksimaalselt viieks aastaks. Andmetöötlejate seisukohast on sertifitseerimisel ja heakskiidetud toimimisjuhendi kasutamisel signaliseeriv

[40] Üldmääruse põhjenduspunkti 26 kohaselt ei tuleks andmekaitse põhimõtteid kohaldada anonüümse teabe suhtes, st teabe suhtes, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga, ega isikuandmete suhtes, mis on muudetud anonüümseks sellisel viisil, et andmesubjekti ei ole võimalik tuvastada.
[41] Erialaliitude loetelu: https://www.eesti.ee/est/kontaktid/erialaliidud_1 (31.01.2017).

efekt – selle kaudu saab tõendada andmesubjektidele (nt klientidele) toodete või teenuste andmekaitse taset ja seega suurendada isikuandmete töötlemisega seotud usaldusväärsust. Teisest küljest saab sertifitseerimisega tõendada üldmääruse erinevate sätete järgimist ja nõuetele vastavust. Andmetöötleja tegevusele saab anda andmekaitse sertifikaadi maksimaalselt kolmeks aastaks.

Muudatustel on tervikuna positiivne mõju ka andmesubjektidele – paremini on tagatud nende õigus isikuandmete kaitsele ning isikuandmetega seotud rikkumistele reageerimine. Nõuete efektiivne rakendamine avaliku võimu kandjate poolt suurendab elanike üldist usaldust avalikus sektoris toimuva andmetöötluse vastu.

6.3. Andmekaitse Inspektsiooni tegevusega seotud muudatused

Eestis määratakse sõltumatuks järelevalveasutuseks üldmääruse artikli 51 mõistes Andmekaitse Inspektsioon (eelnõu § 50), kes vastutab määruse kohaldamise järelevalve eest, et kaitsta füüsiliste isikute põhiõigusi ja -vabadusi seoses nende isikuandmete töötlemisega ning hõlbustada isikuandmete vaba liikumist liidus. Andmekaitse Inspektsiooni tegevust mõjutab hulk muudatusi:

a) Täpsustatakse ja täiendatakse loetelu Andmekaitse Inspektsiooni ülesannetest (vt tabel 7). Lisaks sätestavad eelnõu § 55 lõiked 2 ja 3 täiendavad pädevused eelnõu raames reguleeritu osas.

Tabel 7. Andmekaitse Inspektsiooni ülesanded kehtiva ja uue regulatsiooni valguses

Kehtiv regulatsioon (IKS § 33 lg 1)	**Uus regulatsioon (artikkel 57)**
Andmekaitse Inspektsioon: • kontrollib IKS-is sätestatud nõuete täitmist; • rakendab haldussundi; • algatab väärteomenetluse ja kohaldab karistust; • teeb koostööd välisriikide pädevate asutustega; • annab soovituslikke juhiseid; • täidab muid seadusest tulenevaid ülesandeid.	• Jälgib määruse kohaldamist ja tagab selle; • suurendab üldist teadlikkust töötlemise ohtudest, normidest, kaitsemeetmetest ja õigustest; • nõustab parlamenti, valitsust ja teisi institutsioone; • edendab andmetöötlejate teadlikkust; • annab andmesubjektile teavet tema õiguste kohta; • käsitleb ja menetleb andmesubjekti nimel esitatud kaebusi; • teeb koostööd teiste järelevalveasutustega; • toimetab uurimisi määruse kohaldamise kohta; • jälgib suundumusi, mis mõjutavad isikuandmete kaitset (info- ja sidetehnoloogiad, kaubandustavad); • võtab vastu vastutavat ja volitatud töötlejat omavahel siduva lepingu tüüptingimused ning standardsed andmekaitseklauslid andmete edastamiseks asjakohaste kaitsemeetmete kohaldamisel; • koostab ja avalikustab töötlemistoimingute

tüüpide loetelu, mille puhul on andmekaitsealane mõjuhinnang kohustuslik;
- eelneva konsulteerimise käigus annab nõu seoses kavandatud isikuandmete töötlemisega;
- ergutab toimimisjuhendite koostamist ja kiidab heaks toimimisjuhendite kavandid;
- ergutab andmekaitse sertifikaatide kehtestamist ja kiidab heaks sertifitseerimise kriteeriumid;
- vaatab korrapäraselt läbi AKI väljastatud sertifikaadid;
- koostab ja avaldab toimimisjuhendite järelevalvet teostava asutuse ja sertifitseerimisasutuse akrediteerimise tingimused;
- akrediteerib toimimisjuhendite järelevalvet teostavad asutused ja sertifitseerimisasutused;
- kinnitab lepinguklauslid või -sätted, millega sätestatakse asjakohased kaitsemeetmed isikuandmete edastamiseks kolmandatesse riikidesse;
- kiidab heaks kontsernisisesed eeskirjad;
- panustab andmekaitsenõukogu tegevusse;
- peab registrit määruse rikkumiste ja võetud meetmete kohta;
- täidab mis tahes muid isikuandmete kaitsega seotud ülesandeid.

b) Kuna andmekaitsespetsialisti määranud vastutaval või volitatud töötlejal tekib kohustus teavitada sellest järelevalveasutust, siis tuleb AKI-l lisaks tabelis 7 loetletud ülesannetele ka registreerida andmekaitsespetsialistide kontaktandmed.
c) AKI teostab riiklikku ja haldusjärelevalvet isikuandmete töötlemiseks kehtestatud nõuete üle. Täiendatakse loetelu AKI poolt kohaldatavatest riikliku järelevalve erimeetmetest (lisanduvad viibimiskeeld, vallasasja hoiulevõtmine ja hoiulevõetud vallasasja müümine või hävitamine) ning riikliku järelevalve erisusena sätestatakse üldmääruse artiklis 58 loetletud uurimisvolitused.
d) Reguleeritakse liikmesriikide järelevalveasutuste omavahelist koostööd, vastastikust abistamist ja ühisoperatsioone, et tagada määruse ühetaoline ja efektiivne kohaldamine Euroopa Liidus (artiklid 60–62).
e) Andmekaitse Inspektsioonile kaasneb kohustus teha koostööd Euroopa Andmekaitsenõukoguga, sh teatud juhtudel saata kinnitamiseks enda otsuste eelnõusid ja muud asjakohast teavet (vt artikkel 64).
f) Sunniraha määr, mida võib AKI ettekirjutuse täitmata jätmise korral rakendada, suureneb 20 000 000 euroni või ettevõtja puhul kuni 4% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.

g) Võrreldes kehtiva IKS-iga suurenevad oluliselt isikuandmete töötlemisega seotud rikkumiste eest määratavad karistused (vt tabel 8). Kehtiva IKS-i kohaselt saab isikuandmete töötlemise nõuete rikkumise eest karistada füüsilist isikut rahatrahviga kuni 1200 eurot ning juriidilist isikut kuni 32 000 eurot. AKI peab tagama, et trahvi määramine oleks tõhus, proportsionaalne ja heidutav. Määrus sätestab konkreetsed aspektid, mida järelevalveasutus peab kaaluma karistuse üle otsustamisel.

Tabel 8. Vastutus üldmääruse nõuete rikkumise eest

Rikkumine	**Artiklid**	**Trahv füüsilisele isikule (eurod)**	**Trahv juriidilisele isikule**
Vastutava või volitatud töötleja kohustuste rikkumine	8, 11, 25–39, 42, 43	kuni 10 000 000	kuni 10 000 000 eurot või kuni 2% aastakäibest
Sertifitseerimise korra rikkumine	42, 43	kuni 10 000 000	kuni 10 000 000 eurot või kuni 2% aastakäibest
Toimimisjuhendi järgimise üle järelevalve teostamise korra rikkumine	art 41 lg 4	kuni 10 000 000	kuni 10 000 000 eurot või kuni 2% aastakäibest
Isikuandmete töötlemise põhimõtete rikkumine, sh andmesubjekti nõusoleku andmise korra rikkumine	5– 7, 9	kuni 20 000 000	kuni 20 000 000 eurot või kuni 4% aastakäibest
Andmesubjekti õiguste rikkumine	12–22	kuni 20 000 000	kuni 20 000 000 eurot või kuni 4% aastakäibest
Isikuandmete edastamise korra rikkumine	44–49	kuni 20 000 000	kuni 20 000 000 eurot või kuni 4% aastakäibest
Isikuandmete töötlemise korra rikkumine eriolukordades	eelnõu §-d 4–7	kuni 20 000 000	kuni 20 000 000 eurot või kuni 4% aastakäibest
Andmekaitse inspektsiooni korralduse täitmata jätmine	art 58 lg 2	kuni 20 000 000	kuni 20 000 000 eurot või 4% aastakäibest
Andmekaitse inspektsiooni juurdepääsu võimaldamise rikkumine	art 58 lg 1	kuni 20 000 000	kuni 20 000 000 eurot või 4% aastakäibest

Sihtrühm I – Andmekaitse Inspektsioon
Mõju riigiasutuste korraldusele, kuludele ja tuludele

Mõju AKI-le on peamiselt töökorralduslik, kuid tulenevalt suurenevast töökoormusest kasvavad ka kulud. AKI-s töötab praegu 18 ametnikku, sh peadirektor.

AKI on hinnanud, et asutuse töökoormus hüppab üles eelkõige uue andmekaitseõiguse rakendamise eel ning sellele järgnevalt. Koormus tuleneb eelkõige selgitus- ja teavitustööst,

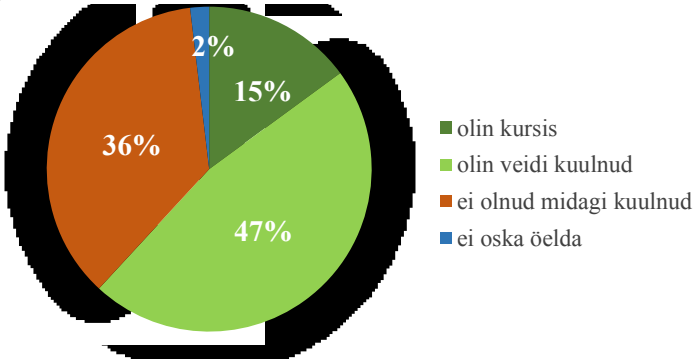
samuti rikkumisteadete käitlemisest, andmekaitsespetsialistide registreerimisest ning väärteomenetluste läbiviimisest. Töökoormusega toimetulekuks on vähendatud ajutiselt omaalgatusliku järelevalvetöö mahtu ning plaanitakse uuendada infosüsteemi.[42] AKI prognoosib enda kuludeks seoses üldmääruse rakendamisega 18 kuu jooksul kokku üle 112 000 euro, mis sisaldab kahe täistöökoormusega ametikoha personalikulusid, majandamiskulusid ja välislähetusi.

Tabel 9. Isikuandmete kaitse üldmääruse rakendamise prognoositavad kulud Andmekaitse Inspektsioonile, 2018–2019 (eurod)

	2018 (12 kuud)	2019 (6 kuud)	Kokku (18 kuud)
Personalikulud	61 013	30 506	91 519
Majandamiskulud	10 840	10 320	21 160
Kokku	71 853	40 826	112 679

AKI on juba praegu enda veebilehel kättesaadavaks teinud suure hulga informatsiooni, mis puudutab uue andmekaitseõigusega kaasnevaid peamisi muudatusi, abistamaks isikuandmete töötlejaid uue regulatsiooniga ettevalmistumisel. Koostatud on juhendmaterjale, mis aitavad andmetöötlejatel hinnata, millised andmekaitsealased kohustused neile rakenduvad, ning AKI ja kõrgkoolide omavahelises koostöös on välja töötatud spetsiaalsed andmekaitsespetsialisti täiendkoolituse programmid.

Siiski tuleb nentida, et enamiku andmetöötlejate teadlikkus andmekaitsereformist on endiselt madal. Probleem ilmneb nii erasektoris, kus ligikaudu kolmandik ettevõtjatest ei ole kevadel jõustuvast andmekaitsereformist midagi kuulnud (joonis 4), aga ka avalikus sektoris. Täpsed andmed avaliku sektori asutuste valmisoleku kohta puuduvad, kuid ministeeriumid on rõhutanud vajadust suurendada oma haldusala teadlikkust selles vallas. AKI hinnangul kasvas nende poole pöördumiste arv juba 2017. aastal ning lähiajal on oodata pöördumiste arvu veelgi suuremat tõusu[43].



Joonis 4. Ettevõtjate teadlikkus andmekaitsereformist (vastused küsimusele „*Kui palju te teadsite enne käesoleva ankeedi täitmist kevadel jõustuvast andmekaitsereformist*?“)
Allikas: Turu-uuringute AS

[42] Andmekaitse Inspektsioon on selgitanud uue andmekaitseõiguse rakenduskulusid ja võimalikke riske: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/memo-rakenduskulud.pdf (13.11.2017).
[43] https://geenius.ee/uudis/andmekaitse-inspektsiooni-statistika-naitab-et-eestlased-tunnevad-suurt-huvi-isikuandmete-kaitse-vastu/ (15.01.2018).

Üksnes 15% ettevõtjatest leiab, et nad on andmekaitsereformiga kursis, ning tervelt 36% tunnistavad, et nad ei ole selle kohta midagi kuulnud. Positiivselt eristuvad suuremad (üle 10 töötajaga) ettevõtted, kus teadlikkus on oluliselt parem võrreldes väikeste ettevõtetega. Näiteks 54% rohkem kui 50 töötajaga ettevõtetest peab ennast andmekaitsereformiga kursis olevaks ning mitte keegi ei märkinud, et ei oleks andmekaitsereformist midagi kuulnud. Tegevusalade lõikes on teadlikkus oluliselt parem info ja side valdkonnas ning kutse-, teadus- ja tehnikaalase tegevusega tegelevates ettevõtetes. Teadlikkus on madalaim tööstusettevõtete hulgas (põllumajandus, mäetööstus, töötlev tööstus, ehitus jm), kus 49% vastajatest ei olnud andmekaitsereformist midagi kuulnud. Paraku puuduvad usaldusväärsed andmed hindamaks, milline on teadlikkus valitsemissektori andmetöötlejate hulgas, kuid võib eeldada, et teadlikkus on kõrgem ministeeriumides ja riigiasutustes ning madalam kohaliku omavalitsuse tasandil.

Muudatuste mõju AKI-le kui sihtrühmale on HÕNTE § 46 mõistes oluline: mõju avaldub sageli (igapäevatöö käigus) ning on ulatuslik – kohanemine eeldab suunatud ja planeeritud tegevusi pikema perioodi vältel. Ebasoovitvaks riskiks on töökoormuse kasv oodatust suuremas ulatuses, mille tagajärjel võib halveneda järelevalve või muude ülesannete kvaliteet. Muudatuste mõju mõnevõrra väheneb kohanemisperioodi möödudes.

Sihtrühm II – isikuandmete töötlejad
Majanduslik mõju: ettevõtluskeskkond ja ettevõtete tegevus

Isikuandmete töötlejad peavad senisest enam koostööd tegema AKI-ga. Näiteks teavitama AKI-t andmekaitsespetsialisti määramisest, teatud juhtudel küsima luba isikuandmete edastamiseks kolmandasse riiki, andma teada isikuandmetega seotud rikkumistest jm. Üheks enim kõneainet pakkunud muudatuseks on aga andmekaitsealaste rikkumiste eest määratavate trahvide suurenemine (kõrgendatud ülemmääraga rahatrahvid).

Millised mõjud kaasnevad selle muudatusega praktikas, ei ole võimalik prognoosida, kuid on tõenäoline, et trahvisummad võrreldes praegusega suurenevad. Siiani on AKI kui kohtuvälise menetleja poolt määratud rahatrahvid olnud suhteliselt väikesed – 2015. aastal määrati väärteotrahv 14 korral, neist suurim trahvisumma oli 160 eurot, väikseim 16 eurot. Algatatud väärteomenetlused puudutasid kohalike omavalitsuste veebilehti (avalikku dokumendiregistrit), meditsiinitöötajaid, kes vaatasid ilma õigusliku aluseta isikute terviseandmeid tervise infosüsteemis ning politsei infosüsteemi ja rahvastikuregistri väärkasutamist.[44] Arvestades, et uus andmekaitseregulatsioon on senisest oluliselt detailsem ning andmesubjekti õigusi rohkem kaitsev, siis võib suureneda ka rikkumiste arv ning väärteomenetluste hulk. 2016. aastal esitati AKI-le 390 kaebust, vaiet või väärteoteadet (tabel 10).

Tabel 10. AKI järelevalvetöö statistika, 2012–2016[45]

	2012	2013	2014	2015	2016
Ringkirjad (ilma järelevalvet algatamata)				5	5
Võrdlevad seired	4	4	6	14	9

[44] AKI ülevaade „Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2015. aastal“ http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf (14.11.2017).
[45] Andmed Andmekaitse Inspektsiooni veebilehelt: http://www.aki.ee/et/inspektsioon/statistika (14.11.2017).

Kaebused, vaided, väärteoteated (esitatud)	404	550	413	446	390
Omaalgatuslikud järelevalveasjad (algatatud)	191	171	152	384	86
Kontrollkäigud (järelevalves)	23	15	48	35	33
Soovitused ja ettepanekud (järelevalves)				299	56
Ettekirjutused (reeglina eelneb ettepanek; reeglina sisaldab sunniraha hoiatust)	187	120	86	77	59
Väärteoasjad (lõpetatud)	43	29	11	16	16
Määratud trahvid ja rakendatud sunniraha	39	22	8	15	16

Muudatuste mõju isikuandmete töötlejatele on enamasti vähese ulatusega, st kohanemine on kerge ja ei vaja spetsiaalseid ümberkorraldusi. Erandiks on olukorrad, kus rikkumise menetlemiseks algatatakse väärteomenetlus, mis võib päädida kõrgendatud ülemmääraga rahatrahvi määramisega. Andmetöötlejatel, kes määravad andmekaitsespetsialisti, on andmekaitsespetsialist esmaseks ja peamiseks kontaktpunktiks suhtlemisel AKI-ga, seetõttu on andmekaitsespetsialisti määramine soovituslik ka neile, kellel selleks otsest kohustust ei ole.

6.4. Mõju õiguskaitseasutustele

Muudest andmetöötlejatest eraldi käsitletakse andmekaitsereformi mõju õiguskaitseasutustele, kuivõrd isikuandmete töötlemist süütegude tõkestamisel, avastamisel, menetlemisel ja karistuste täideviimisel ei hakka reguleerima mitte üldmäärus, vaid eelnõu kolmas peatükk. Sellega võetakse üle direktiiv 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist. Tuleb rõhutada, et eelnõu kolmas peatükk ei kohaldu isikuandmete töötlemisele riikliku järelevalve teostamisel.

Olulisemad muudatused võrreldes praegu süütegude menetlemisele kehtiva regulatsiooniga on järgmised:

a) Isikuandmete säilitamise tähtaja kehtestamine. Isikuandmeid tohib isikustatud kujul säilitada üksnes seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks andmed koguti.
b) Isikuandmete eri kategooriate eristamine ning hinnangutel põhinevate isikuandmete eristamine.
c) Sätestatakse andmesubjekti õigus teabele (kättesaadavaks tehtav teave, teavitamisel antav teave, andmesubjekti nõudmisel esitatav teave) ning õigus isikuandmete parandamisele ja kustutamisele. Võrreldes üldmäärusega on jäetud rohkem ruumi nende õiguste piiramiseks tulenevalt valdkonna eripärast.
d) Andmetöötleja kohustus lõimitud ja vaikimisi andmekaitseks.
e) Sätestatakse sõnaselgelt, milliste isikuandmete töötlemise toimingute kohta tuleb pidada logisid.
f) Isikuandmete töötlemise toimingute registreerimine.
g) Andmekaitselise mõjuhinnangu kohustus ja eelnev konsulteerimine AKI-ga.
h) Andmekaitsespetsialisti määramise kohustus kõigile õiguskaitseasutustele.
i) AKI ja andmesubjekti teavitamine isikuandmetega seotud rikkumisest.
j) Reguleeritakse isikuandmete edastamist kolmandale riigile või rahvusvahelisele organisatsioonile. Teatud juhtudel kaasneb edastamisega kohustus teavitada AKI-t.

Uue IKS-i jõustumisel muutub süütegudega seotud isikuandmete töötlemine senisest reguleeritumaks, samas on nõuded mõnevõrra leebemad kui üldmääruse kohaldamisalas. Eestis tegelevad süütegude menetlemise ja karistuse täideviimisega järgmised asutused:

- Andmekaitse Inspektsioon
- Finantsinspektsioon
- I ja II astme kohtud
- Justiitsministeerium
- Kaitsepolitseiamet
- Kaitseressursside Amet
- Kaitsevägi
- Keeleinspektsioon
- Keskkonnainspektsioon
- kohalikud omavalitsused
- Konkurentsiamet
- Lennuamet
- Maanteeamet
- Maksu- ja Tolliamet
- Politsei- ja Piirivalveamet
- Prokuratuur
- Põllumajandusamet
- Päästeamet
- Rahandusministeerium
- Ravimiamet
- Riigikohus
- Tarbijakaitseamet
- Tehnilise Järelevalve Amet
- Terviseamet
- Tööinspektsioon
- Veeteede Amet
- Veterinaar- ja Toiduamet
- vanglad ja kriminaalhooldusosakonnad
- Muinsuskaitseamet

Õiguskaitseasutuste andmetöötluse oluliseks erinevuseks võrreldes üldmääruse kohaldamisalasse jääva töötlusega on kohustus eristada asjakohasel juhul andmesubjektide kategooriaid. Eristada tuleb menetlusaluseid isikuid, kahtlustatavaid, süüdistatavaid, kannatanuid ja tunnistajaid. Tegemist on muudatusega, mis võib vajada täiendavaid IT-arendusi õiguskaitseasutuste poolt kasutatavates infosüsteemides.

Uueks nõudeks on ka faktidel põhinevate isikuandmete eristamine isiklikel hinnangutel põhinevatest andmetest. Muudatuse rakendamisel on esmatähtis, et andmeid töötlevad inimesed oleksid informeeritud ja teadlikud uuest nõudest. Ka andmesubjekti õigusi puudutavad muudatused on oma olemuselt pigem töökorralduslikud ning nende rakendamisega kaasnevaid kulusid ei saa pidada märkimisväärseks: näiteks sätestatakse seaduses, milline andmekaitset puudutav teave tuleb andmesubjektile kergesti juurdepääsetaval viisil avalikuks teha (nt asutuse veebilehel) ning milline teave andmesubjekti soovil talle anda. Võrreldes üldmäärusega jätab seadus õiguskaitseasutustele rohkem kaalutlusruumi andmesubjekti õiguste piiramisel.

Isikuandmete töötlemist süütegude tõkestamisel, avastamisel, menetlemisel ja karistuse täideviimisel puudutavad muudatused kattuvad suures osas üldmäärusega ning nende mõju õiguskaitseasutustele on üldjoontes samasugune kui teistele avaliku sektori andmetöötlejatele (vt punktid 6.1 ja 6.2).

Kuna suur osa isikuandmete töötlemisest toimub elektrooniliselt, siis tuleb seaduse rakendamisel erilist tähelepanu pöörata infosüsteemide arendamisele. See puudutab näiteks isikuandmete kustutamist säilitustähtaja saabudes, andmesubjektide eri kategooriate eristamist ning logide pidamise kohustust. Muudatustega kaasneb vähemalt järgmiste infosüsteemide arendamise vajadus:

- kriminaalmenetluse register;
- vangiregister;
- kinnipeetavate isikute register;

- väärteomenetluse portaal/e-toimiku väärteomenetluse liides;
- kohtueksperti infosüsteem;
- jälitustoimingute infosüsteem.

Sihtrühmadele kaasnev mõju on enamiku muudatuste puhul töökorralduslikku laadi. Otsene rahaline kulu tuleneb infotehnoloogiliste arenduste vajadusest ning seoses andmekaitsespetsialisti regulatsiooniga (palga-, majandus- ja koolituskulud, atesteerimine). Ühe andmekaitsespetsialisti iga-aastaseks kuluks on eelnõu koostaja hinnanud keskmiselt 30 000 – 35 000 eurot, kuid tulenevalt palgatasemest võib kulu olla keskmisest suurem Tallinna ja Harjumaa piirkonnas.

Mõju võib tervikuna hinnata oluliseks – mõju ulatus ja sihtrühma suurus on keskmised, kuid mõju avaldub sageli (regulaarselt). Regulatsioon suurendab vähesel määral õiguskaitseasutuste töökoormust.

7. Rakendamisega seotud kulud

Andmekaitse Inspektsioon on prognoosinud enda täiendavateks kuludeks seoses uue andmekaitseõiguse rakendamisega 112 679 eurot järgneva kahe aasta jooksul. Kui ilmneb, et inspektsiooni töökoormuse kasv on püsiv, siis tõenäoliselt kasvavad asutuse kulud ka järgnevatel aastatel.

Teiseks oluliseks rakendamisega seotud kuluks on andmekaitsespetsialisti regulatsiooniga kaasnevad kulud. Suurest määramatusest tulenevalt ei ole võimalik kogukulu usaldusväärselt hinnata – avaliku võimu kandjad võivad mitme asutuse peale määrata ühise andmekaitsespetsialisti, samuti võivad kõik andmetöötlejad teenust sisse osta või määrata andmekaitsespetsialistiks juba olemasoleva töötaja või üksuse. Oluliseks kuluks andmetöötlejatele on ka koolituskulud, olenemata sellest, kas andmekaitsespetsialist määratakse või mitte.

Kolmas kulude aspekt seondub infotehnoloogiliste arenduste vajadusega. Tervikpilti kuludest ei ole võimalik ka siinkohal prognoosida, sest muudatused puudutavad suurt hulka avalikus ja erasektoris kasutusel olevatest andmekogudest ja infosüsteemidest.

8. Rakendusaktid

Kõnesoleva eelnõuga ei ole ette nähtud rakendusaktide koostamist.

9. Seaduse jõustumine

Seadus jõustub määrusega ühel ajal ehk 25. mail 2018. Üldmääruse jõustumine 25. mail 2018 on ette nähtud määruse art 99 lg-s 2. Direktiivi 2016/680 ülevõtmiseks peavad liikmesriigid kehtestama vajalikud riigisisesed normid 6. maiks 2018 (direktiivi art 63 lg 1). Kuigi direktiivi ülevõtmiseks kehtestatavad riigisisesed normid peaksid olema jõustunud 19 päeva varem, kui rakendatakse üldmääruse rakendamist, on Eesti hinnangul asjakohane kogu reeglistiku üheaegne rakendamine, eeskätt tulenevalt direktiivi ja määruse kohaldamisala piiritlemise keerukusest, valdkonna komplekssusest ja IKS-i terviklikkusest.

10. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon.

Eelnõu saadeti kooskõlastamiseks ministeeriumidele ja arvamuse avaldamiseks järgmistele asutustele ja organisatsioonidele:
1) Õiguskantsleri Kantselei;
2) Riigikohus;
3) Andmekaitse Inspektsioon;
4) Tarbijakaitseamet;
5) Eesti Linnade Liit;
6) Eesti Maaomavalitsuste Liit;
7) MTÜ Lastekaitse Liit;
8) SA Kutsekoda;
9) Pangaliit;
10) Tartu Ülikooli õigusteaduskond;
11) Tallinna Tehnikaülikooli õiguse instituut;
12) Tallinna Ülikooli õigusakadeemia;
13) Eesti Infotehnoloogia ja Telekommunikatsiooni Liit;
14) Eesti E-Kaubanduse Liit;
15) Eesti Haiglate Liit;
16) Eesti Kaupmeeste Liit;
17) Eesti Kindlustusseltside Liit;
18) Eesti Turvaettevõtete Liit;
19) Eesti Ajakirjanike Liit;
20) Riigiprokuratuur;
21) Registrite ja Infosüsteemide Keskus;
22) Politsei ja Piirivalveamet;
23) Eesti Kohtuekspertiisi Instituut;
24) Eesti Advokatuur.

Kooskõlastamise tulemused on esitatud käesoleva seletuskirja lisas 2.

Algatab Vabariigi Valitsus