



17/ET

WP 248 rev. 01

**Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist,
kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt
määrusele (EL) 2016/679**

Vastu võetud 4. aprillil 2017

Viimati muudetud ja muudatused vastu võetud 4. oktoobril 2017

Töörühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Tegemist on Euroopa sõltumatu nõuandeorganiga andmekaitse ja eraelu puutumatuse küsimustes. Töörühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaaditeenused tagab Euroopa Komisjoni õigusküsimuste peadirektoraadi direktoraat C (põhiõigused ja liidu kodakondsus), B-1049 Brüssel, Belgia, kabinet nr MO-59 03/075.

Veebisait: http://ec.europa.eu/justice/data-protection/index_en.htm.

TÖÖRÜHM ÜKSIKISIKUTE KAITSEKS SEOSSES ISIKUANDMETE TÖÖTLEMISEGA,

mis on loodud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiviga 95/46/EÜ,

võttes arvesse nimetatud direktiivi artikleid 29 ja 30,

võttes arvesse oma töökorda,

ON VASTU VÕTNUD KÄESOLEVAD SUUNISED:

Sisukord

I.	SISSEJUHATUS.....	4
II.	SUUNISTE KOHALDAMISALA.....	5
III.	ANDMEKAITSEALANE MÕJUINNANG: MÄÄRUS LAHTISELETATUNA	7
A.	MIDA ANDMEKAITSEALASES MÕJUINNANGUS KÄSITLETAKSE? ÜKSIKUT ISIKUANDMETE TÖÖTLEMISE TOIMINGUT VÕI SARNASEID ISIKUANDMETE TÖÖTLEMISE TOIMINGUID.	8
B.	MILLISTE ISIKUANDMETE TÖÖTLEMISE TOIMINGUTE PUHUL NÕUTAKSE ANDMEKAITSEALAST MÕJUINNANGUT? KUI ERANDID KÕRVALE JÄTTA, SIIS SELLISTE PUHUL, MILLE TULEMUSENA „TEKIB TÕENÄOLISELT SUUR OHT“	9
a)	Millal on andmekaitsealane mõjuhinna kohustuslik? Siis, kui isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“.	9
b)	Millal ei nõuta andmekaitsealast mõjuhinna? Siis, kui isikuandmete töötlemise tulemusena ei teki tõenäoliselt suurt ohtu, kui sarnane andmekaitsealane mõjuhinna on juba olemas, kui isikuandmete töötlemiseks on antud luba enne 2018. aasta maid, kui isikuandmete töötlemisel on õiguslik alus või kui isikuandmete töötlemine on nende töötlemistoimingute loetelus, mille puhul andmekaitsealast mõjuhinna ei nõuta.	14
C.	KUIDAS ON LOOD JUBA KÄSILOLEVATE ISIKUANDMETE TÖÖTLEMISE TOIMINGUTEGA? TEATAVATEL ASJAOLUDEL ON NÕUTAV ANDMEKAITSEALANE MÕJUINNANG.	15
D.	KUIDAS TEHA ANDMEKAITSEALANE MÕJUINNANG?	16
a)	Millal tuleks andmekaitsealane mõjuhinna teha? Enne isikuandmete töötlemist.	16
b)	Kes on kohustatud tegema andmekaitsealase mõjuhinna? Vastutav töötleja koos andmekaitseametniku ja volitatud töötlejatega.	16
c)	Millist metoodikat tuleks rakendada andmekaitsealase mõjuhinna tegemisel? Metoodikad on erinevad, kuid kriteeriumid on ühised.	17
d)	Kas on olemas kohustus andmekaitsealane mõjuhinna avaldada? Ei, kuid kokkuvõtte avaldamine võib suurendada usaldust ning eelneva konsulteerimise või andmekaitseasutuse taotluse korral tuleb andmekaitsealane mõjuhinna tervikuna edastada järelevalveasutusele.	20
E.	MILLAL TULEKS KONSULTEERIDA JÄRELEVALVEASUTUSEGA? SIIS, KUI JÄÄKRISKID ON SUURED.	20
IV.	JÄRELDUSED JA SOOVITUSED	21
1. LISA.	ELI ANDMEKAITSEALASE MÕJU HINDAMISE KEHTIVATE RAAMISTIKE NÄITED	23
2. LISA.	ANDMEKAITSEALASE MÕJUINNANGU KRITEERIUMID.....	24

I. Sissejuhatus

Alates 25. maist 2018 hakatakse kohaldama määrust (EL) 2016/679¹ (isikuandmete kaitse üldmäärus). Isikuandmete kaitse üldmääruse artikliga 35 on võetud kasutusele andmekaitsealase mõjuhinnangu mõiste,² mis on sätestatud ka direktiivis 2016/680³.

Andmekaitsealase mõjuhinnangu eesmärk on kirjeldada isikuandmete töötlemist, hinnata selle vajalikkust ja proportsionaalsust ning aidata käsitleda selle tulemusena füüsiliste isikute õigustele ja vabadustele tekkivaid ohte⁴ neid ohte hinnates ja määrares kindlaks meetmed, mille abil neid ohte käsitleda. Andmekaitsealane mõjuhinnang on oluline vahend vastutuse vaatenurgast, sest see mitte üksnes ei aita vastutavatel töötajatel täita isikuandmete kaitse üldmääruse nõudeid, vaid aitab ka tõendada seda, et määrusega kooskõla tagamiseks on võetud asjakohased meetmed (vt ka artikkel 24)⁵. Teisisõnu on **andmekaitsealase mõjuhinnangu tegemine protsess, millega tagatakse vastavus ja tõendatakse seda**.

Vastavalt isikuandmete kaitse üldmäärusele võib andmekaitsealase mõjuhinnangu nõuete täitmata jätmine kaasa tuua pädeva järelevalveasutuse määratavad trahvid. Andmekaitsealase mõjuhinnangu tegematajätmine juhul, kui seda isikuandmete töötlemisega seoses nõutakse (artikli 35 lõiked 1, 3 ja 4), andmekaitsealase mõjuhinnangu tegemine ebaõigel viisil (artikli 35 lõige 2 ja lõiked 7–9) või pädeva järelevalveasutusega konsulteerimata jätmine olukorras, kus seda nõutakse (artikli 36 lõike 3 punkt e), võib kaasa tuua haldustrahvi, mille suurus on kuni 10 miljonit eurot või ettevõtja puhul kuni

¹ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

² Muus kontekstis kasutatakse samale mõistele osutamisel sageli mõistet „eraelu puutumatusse avalduva mõju hinnang“.

³ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (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) artiklis 27 on samuti sätestatud, et kui isikuandmete töötlemise tulemusena „*tekib füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht*“, on vaja hinnata eraelu puutumatusse avalduvat mõju.

⁴ Isikuandmete kaitse üldmääruses ei ole andmekaitsealase mõjuhinnangu mõistet määratletud,

- kuid andmekaitsealase mõjuhinnangu miinimumsisu on kindlaks määratud artikli 35 lõikes 7:
 - o „a) kavandatud isikuandmete töötlemise toimingute ja töötlemise eesmärkide, sealhulgas asjakohasel juhul vastutava töötleja õigustatud huvi süstemaatiline kirjeldus;
 - o b) isikuandmete töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine eesmärkide suhtes;
 - o c) lõikes 1 osutatud andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnang ning
 - o d) ohtude käsitlemiseks kavandatud meetmed, sealhulgas tagatised, turvameetmed ja mehhanismid isikuandmete kaitse tagamiseks ja käesoleva määruse järgimise tõendamiseks, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.“;
- andmekaitsealase mõjuhinnangu tähendust ja rolli on selgitatud põhjenduses 84: „*Käesoleva määruse järgimise parandamiseks juhtudel, kus isikuandmete töötlemise toimingud kujutavad endast füüsiliste isikute õigustele ja vabadustele tõenäoliselt suurt ohtu, peaks vastutav töötleja vastutama andmekaitsealase mõjuhinnangu tegemise eest, et hinnata eelkõige selle ohu päritolu, laadi, eripära ja tõsidust.*“

⁵ Vt ka põhjendus 84: „*Hinnangu tulemust tuleks arvestada asjakohaste meetmete kindlaksmääramisel, mis tuleb võtta selle tõendamiseks, et isikuandmete töötlemine on käesoleva määrusega kooskõlas.*“

2 % tema eelneva majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb summa on suurem.

II. Suuniste kohaldamisala

Suunistes on arvesse võetud

- artikli 29 alusel asutatud andmekaitse töörühma (edaspidi „artikli 29 töörühm“) hinnangut, mis käsitleb riskipõhise lähenemisviisi rolli isikuandmete kaitse õigusraamistikes (14/EN WP 218)⁶;
- artikli 29 töörühma suuniseid andmekaitseametnike kohta (16/EN WP 243)⁷;
- artikli 29 töörühma arvamust eesmärgi piirangu kohta (13/EN WP 203)⁸;
- rahvusvahelisi standardeid⁹.

Kooskõlas isikuandmete kaitse üldmääruses sätestatud riskipõhise lähenemisviisiga ei ole andmekaitsealase mõjuhinna koostamine kohustuslik iga isikuandmete töötlemise toimingu puhul. Andmekaitsealast mõjuhinna koostamist nõutakse vaid juhul, kui isikuandmete töötlemise tulemusena „*tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht*“ (artikli 35 lõige 1). Selleks et asjaolusid, mille puhul andmekaitsealane mõjuhinna koostamine on kohustuslik (artikli 35 lõige 3), tõlgendataks ühetaoliselt, püütakse käesolevates suunistes seda mõistet selgitada ja sätestada kriteeriumid loetelude jaoks, mille andmekaitseametnikud peavad vastu võtma artikli 35 lõike 4 alusel.

Vastavalt artikli 70 lõike 1 punktile e saab Euroopa Andmekaitsekoogu anda isikuandmete kaitse üldmääruse järjepideva kohaldamise ergutamiseks välja suuniseid, soovitusi ja häid tavaid. Käesoleva dokumendi koostamisel püüti sellist andmekaitsekoogu tulevast tööd ette näha ning seepärast selgitatakse selles isikuandmete kaitse üldmääruse asjakohaseid sätteid, et aidata vastutavatel töötajatel täita seadust ja tagada õiguskindlus neile vastutavatele töötajatele, kes peavad tegema andmekaitsealase mõjuhindangu.

Samuti on käesolevate suuniste eesmärk aidata koostada

- ELi ühine loetelu isikuandmete töötlemise toimingutest, mille puhul andmekaitsealane mõjuhinna on kohustuslik (artikli 35 lõige 4);
- ELi ühine loetelu isikuandmete töötlemise toimingutest, mille puhul andmekaitsealane mõjuhinna ei ole kohustuslik (artikli 35 lõige 5);
- andmekaitsealase mõjuhinna koostamise meetodikat käsitlevad ühised kriteeriumid (artikli 35 lõige 5);

⁶ „Statement on the role of a risk-based approach to data protection legal frameworks“, vastu võetud 30. mail 2014.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532.

⁷ „Guidelines on Data Protection Officers („DPOs“)“, vastu võetud 13. detsembril 2016.

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A.

⁸ „Opinion 03/2013 on purpose limitation“, vastu võetud 2. aprillil 2013.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409.

⁹ Nt Rahvusvaheline Standardiorganisatsioon (ISO), ISO 31000:2009 –riskijuhtimine – põhimõtted ja juhised; Rahvusvaheline Standardiorganisatsioon (ISO), ISO/IEC 29134 (projekt) – infotehnoloogia – turbetehnika – eraelu puutumatusele avalduva mõju hindamine – juhised.

- ühised kriteeriumid selle kindlaksmääramiseks, millal tuleb konsulteerida järelvalveasutusega (artikli 36 lõige 1), ning
- soovitusel, tuginedes võimaluse korral ELi liikmesriikides saadud kogemustele.

III. Andmekaitsealane mõjuhindang: määrus lahtiseletatuna

Isikuandmete kaitse üldmääruse kohaselt peavad vastutavad töötlejad rakendama asjakohaseid meetmeid, et tagada ja suuta tõendada kooskõla isikuandmete kaitse üldmäärusega, võttes muu hulgas arvesse „füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte“ (artikli 24 lõige 1). Vastutavate töötlejate kohustuse puhul teha teatavatel asjaoludel andmekaitsealane mõjuhindang tuleks arvesse võtta nende üldist kohustust käsitleda asjakohaselt isikuandmete töötlemisega kaasnevaid ohte¹⁰.

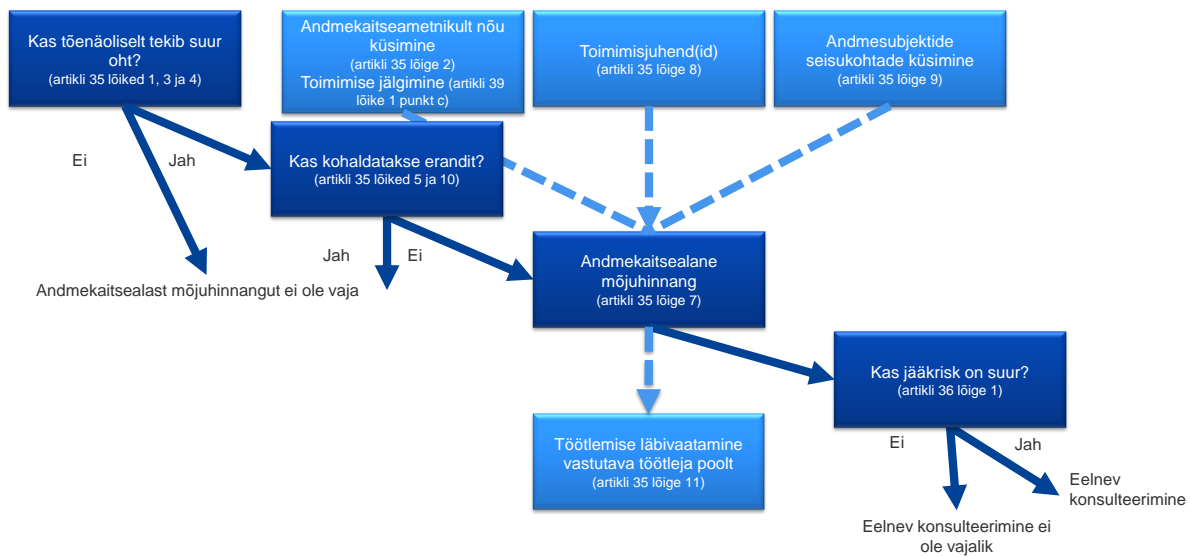
Oht hõlmab sündmust ja selle tagajärgi ning seda hinnatakse suuruse ja tõenäosuse vaatenurgast. Ohtude käsitlemist saab määratleda kui ohtudega seotud kooskõlastatud tegevust organisatsiooni juhtimisel ja kontrollimisel.

Artiklis 35 on osutatud „füüsiliste isikute õigusi ja vabadusi“ ähvardavale tõenäoliselt suurele ohule. Nagu on märgitud artikli 29 tööühma hinnangus, mis käsitleb riskipõhise lähenemisviisi rolli isikuandmete kaitse õigusraamistik, hõlmab viide andmesubjektide õigustele ja vabadustele eeskätt õigust isikuandmete kaitsele ja eraelu puutumatusele, kuid võib hõlmata ka muid põhiõigusi, nagu sõnavabadus, mõttevabadus, liikumisvabadus, diskrimineerimiskeeld, õigus vabadusele ning südametunnistuse- ja usuvabadus.

Kooskõlas isikuandmete kaitse üldmääruses sätestatud riskipõhise lähenemisviisiga ei ole andmekaitsealase mõjuhindangu koostamine kohustuslik iga isikuandmete töötlemise toimingu puhul. Andmekaitsealast mõjuhindangut nõutakse vaid juhul, kui teatava töötlemisviisi rakendamise tulemusena „tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht“ (artikli 35 lõige 1). Ainuüksi asjaolu, et tingimused, mille puhul tekib kohustus teha andmekaitsealane mõjuhindang, ei ole täidetud, ei vähenda siiski vastutavate töötlejate üldist kohustust rakendada meetmeid, et asjakohaselt käsitleda andmesubjektide õigusi ja vabadusi ähvardavaid ohte. Praktikas tähendab see seda, et vastutavad töötlejad peavad pidevalt hindama enda töötlemistegevusest tulenevaid ohte, et teha kindlaks, millal mõne töötlemisviisi rakendamise tulemusena „tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht“.

¹⁰ Tuleb rõhutada, et füüsiliste isikute õigusi ja vabadusi ähvardavate ohtude käsitlemiseks tuleb asjaomased ohud kindlaks teha, neid ohte analüüsida ja hinnata, nende ohtudega tegeleda (nt neid leevendada) ja need ohud läbi vaadata korrapäraselt. Vastutavad töötlejad ei pääse vastutusest, kattes ohud kindlustuslepinguga.

Järgnev joonis kajastab isikuandmete kaitse üldmääruse kohaseid andmekaitsealase mõjuhinna põhiaspekte.



A. Mida andmekaitsealases mõjuhinna käsitletakse? Üksikut isikuandmete töötlemise toimingut või sarnaseid isikuandmete töötlemise toiminguid.

Andmekaitsealane mõjuhinna võib hõlmata üksikut isikuandmete töötlemise toimingut. Samas on artikli 35 lõikes 1 öeldud, et „[e]ndast sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata koos“. Põhjenduses 92 on lisatud, et „[o]n juhtumeid, mille puhul võib olla mõistlik ja säästlik hõlmata andmekaitsealase mõjuhinna rohkem kui üht projekti, näiteks juhul, kui avaliku sektori asutused või organid kavatsevad kasutusele võtta ühise rakenduse või töötlemisplatvormi või mitu vastutavat töötajat kavatseb kasutusele võtta ühise rakenduse või töötlemiskeskonna kogu tööstusharus või allharus või laialdaselt kasutatava horisontaalse tegevuse puhul“.

Mitme laadi, ulatuse, konteksti, eesmärkide ja ohtude poolest sarnase **isikuandmete töötlemise toimingut** hindamiseks võib kasutada üht andmekaitsealast mõjuhinna. Andmekaitsealaste mõjuhinna eesmärk on süstemaatiliselt uurida uusi olukordi, millega võib kaasneda suur oht füüsiliste isikute õigustele ja vabadustele. Ei ole mingit vajadust koostada andmekaitsealane mõjuhinna juhtumite puhul (nt konkreetses kontekstis ja konkreetsel eesmärgil tehtavad isikuandmete töötlemise toimingud), mida on juba uuritud. Nii võib see olla juhul, kui sama liiki andmete samal eesmärgil kogumiseks kasutatakse sarnast tehnoloogiat. Näiteks võib rühm omavalitsusi, kes paigaldavad sarnast videovalvesüsteemi, teha ühe andmekaitsealase mõjuhinna, mis hõlmab nende eraldi vastutavate töötajate tehtavat isikuandmete töötlemist, või võib raudtee-ettevõtja (üks vastutav töötaja) koostada kõikides oma raudteejaamades kasutatava videovalve kohta ühe andmekaitsealase mõjuhinna. Ühe mõjuhinna kasutamine võib olla võimalik ka eri vastutavate töötajate tehtavate sarnaste töötlemistoimingute puhul. Sellistel juhtudel tuleks esitada või teha avalikult kättesaadavaks andmekaitsealase mõjuhinna näidisvorm, viia ellu andmekaitsealases mõjuhinna kirjeldatud meetmed ja esitada põhjendus ühe andmekaitsealase mõjuhinna koostamise kohta.

Kui isikuandmete töötlemise toimingus osalevad kaasvastutavad töötajad, peavad nad täpselt kindlaks määrama oma vastavad kohustused. Nende andmekaitsealases mõjuhinna tuleks kindlaks

määrata, milline osaline vastutab ohtude käsitlemiseks ning andmesubjektide õiguste ja vabaduste kaitsmiseks kavandatud meetmete eest. Iga vastutav töötleja peaks väljendama oma vajadusi ja jagama kasulikku teavet, paljastamata sealjuures saladusi (st kaitsma ärisaladusi, intellektuaalomandit ja konfidentsiaalselt äriteavet) ja avalikustamata nõrku kohti.

Andmekaitsealane mõjuhinnaang võib olla kasulik ka selleks, et hinnata tehnoloogia toote, näiteks tarkvara või riistvara **andmekaitsealast mõju**, kui eri vastutavad töötledjad tõenäoliselt kasutavad seda erinevate töötlemistoimingute tegemiseks. Toodet kasutav vastutav töötledja on loomulikult endiselt kohustatud tegema seoses toote konkreetse kasutusega omaenda andmekaitsealase mõjuhinnaangu, kuid vajaduse korral saaks ta tugineda selle tegemisel andmekaitsealasele mõjuhinnaangule, mille on koostanud toote pakkuja. Selle näiteks võiks olla nutiarvestite tootjate ja kommunaalettevõtjate vaheline suhe. Iga toote pakkuja või isikuandmete töötledja peaks jagama kasulikku teavet, paljastamata sealjuures saladusi ja tekitamata nõrkade kohtade avalikustamisega turvariske.

B. Milliste isikuandmete töötlemise toimingute puhul nõutakse andmekaitsealast mõjuhinnaangu? Kui erandid kõrvale jätta, siis selliste puhul, mille tulemusena „tekib tõenäoliselt suur oht“.

Käesolevas punktis kirjeldatakse, millal on andmekaitsealane mõjuhinnaang kohustuslik ja millal ei ole vaja seda koostada.

Välja arvatud juhul, kui isikuandmete töötlemise toimingu suhtes on kohaldatav mõni erand (III jaotise punkti B alapunkt b), tuleb andmekaitsealane mõjuhinnaang teha, kui isikuandmete töötlemise toimingu tulemusena „tekib tõenäoliselt suur oht“ (III jaotise punkti B alapunkt a).

a) Millal on andmekaitsealane mõjuhinnaang kohustuslik? Siis, kui isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“.

Isikuandmete kaitse üldmääruses ei nõuta andmekaitsealase mõjuhinnaangu koostamist iga isikuandmete töötlemise toimingu puhul, mille tulemusena võib tekkida oht füüsiliste isikute õigustele ja vabadustele. Andmekaitsealase mõjuhinnaangu tegemine on kohustuslik vaid siis, kui töötlemise tulemusena „tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht“ (artikli 35 lõige 1, mis on lahti seletatud artikli 35 lõikes 3 ja mida täiendab artikli 35 lõige 4). See on eriti asjakohane uue andmetöötlustehnoloogia kasutuselevõtu korral¹¹.

Juhul kui ei ole selge, kas andmekaitsealast mõjuhinnaangu nõutakse, soovib artikli 29 töörihm mõjuhinnaangu sellegipoolest koostada, sest see on kasulik vahend, mis aitab vastutavatel töötledjatel järgida andmekaitsealaseid õigusakte.

Ehkki andmekaitsealast mõjuhinnaangu võidakse nõuda ka muudel asjaoludel, on isikuandmete kaitse üldmääruse artikli 35 lõikes 3 esitatud mõned näited selle kohta, millal isikuandmete töötlemise toimingu tulemusena „tekib tõenäoliselt suur oht“:

- „a) füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad

¹¹ Lisanäiteid leiab põhjendustest 89 ja 91 ning artikli 35 lõigetest 1 ja 3.

*otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut*¹²;

- *b) artikli 9 lõikes 1 osutatud andmete eriliikide või artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslik töötlemine*¹³ või
- *c) avalike alade ulatuslik süstemaatiline jälgimine*¹⁴.

Artikli 35 lõike 3 sissejuhatavas lauses kasutatud sõna „eeskätt“ osutab sellele, et see loetelu ei ole täielik. Võib esineda isikuandmete töötlemise toiminguid, mida ei ole selles loetelus nimetatud, kuid mille tulemuseks on samamoodi suur oht. Nende toimingute puhul tuleks samuti teha andmekaitsealane mõjuhindang. Seepärast minnakse allpool kirjeldatud kriteeriumides teinekord kaugemale pelgalt selle selgitamisest, mida tuleks mõista artikli 35 lõikes 3 esitatud kolme näite all.

Selleks et moodustada konkreetsem kogum isikuandmete töötlemise toimingutest, mille puhul nõutakse kaasneva suure ohu tõttu andmekaitsealast mõjuhindangut, võttes arvesse artikli 35 lõike 1 ning artikli 35 lõike 3 punktide a–c konkreetseid elemente, artikli 35 lõike 4 alusel riigi tasandil vastu võetavat loetelu, põhjendusi 71, 75 ja 91 ning muid isikuandmete kaitse üldmääruses esitatud viiteid isikuandmete töötlemise toimingutele, mille tulemusena „*tekib tõenäoliselt suur oht*“,¹⁴ tuleks lähtuda järgmistest kriteeriumidest.

1. Hindamine, sealhulgas profiilianalüüsi tegemine ja prognoosimine, eelkõige „*selliste aspektide analüüsimine ja prognoosimine, mis on seotud töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega*“ (põhjendused 71 ja 91). Näiteks võiks olla finantsasutus, kes kontrollib oma kliente krediidiinfo andmebaasi või rahapesu ja terrorismi rahastamise või pettuse vastu võitlemise andmebaasi põhjal, või biotehnoloogiaettevõtte, mis pakub geeniteste otse tarbijatele, et hinnata ja prognoosida haigus- või terviseriske, või ettevõtja, kes koostab käitumuslikke või turundusprofiile, tuginedes oma veebisaidi kasutamise või vaatamise andmetele.
2. Õiguslike või samaväärsete oluliste tagajärgedega automatiseeritud otsuste tegemine: isikuandmete töötlemine, mille eesmärk on teha andmesubjektide kohta otsuseid, millel on „*füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut*“ (artikli 35 lõike 3 punkt a). Näiteks võib isikuandmete töötlemine kaasa tuua üksikisikute välistamise või diskrimineerimise. Isikuandmete töötlemine, millel on üksikisikutele väike või olematu mõju, ei vasta sellele kriteeriumile. Neid mõisteid selgitatakse põhjalikumalt peagi avaldatavates artikli 29 tööühma suunistes profiilianalüüsi kohta.
3. Süstemaatiline jälgimine: isikuandmete töötlemine, mida kasutatakse andmesubjektide jälgimiseks või kontrollimiseks, sealhulgas andmete kogumine võrgustike kaudu või „*avalike*

¹² Vt põhjendus 71: „*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 profile*“.

¹³ Vt põhjendus 75: „*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*“.

¹⁴ Vt näiteks põhjendused 75, 76, 92 ja 116.

alade ulatuslik süstemaatiline jälgimine“ (artikli 35 lõike 3 punkt c)¹⁵. Seda liiki jälgimine on arvatud kriteeriumide hulka sellepärast, et isikuandmeid võidakse koguda olukorras, kus andmesubjektid ei pruugi olla teadlikud sellest, kes nende andmeid kogub ja kuidas neid kasutatakse. Lisaks ei pruugi üksikisikutel olla võimalik vältida sellist isikuandmete töötlemist avalikel aladel.

4. Tundlikud andmed või väga isiklikud andmed: siia kuuluvad artiklis 9 määratletud eriliiki isikuandmed (nt teave üksikisikute poliitiliste vaadete kohta), samuti artiklis 10 määratletud isikuandmed, mis on seotud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega. Näitena võib tuua üldhaigla, mis säilitab patsientide tervisekaarte, või eraurija, kelle valduses on õigusrikkujate andmed. Väljaspool isikuandmete kaitse üldmääruse sätete kohaldamist võib mõnda liiki isikuandmeid lugeda isikuandmeteks, mille töötlemine suurendab võimalikku ohtu üksikisikute õigustele ja vabadustele. Neid isikuandmeid peetakse tundlikeks (kuna see mõiste on üldiselt arusaadav), sest need on seotud koduse ja isikliku tegevusega (nt elektrooniline suhtlus, mille konfidentsiaalsust tuleks kaitsta), need mõjutavad mõne põhiõiguse kasutamist (nt asukohaandmed, mille kogumisega seatakse kahtluse alla liikumisvabadus) või on nende kuritarvitamisel selgelt tõsine mõju andmesubjekti igapäevaelule (nt finantsandmed, mida võidakse kasutada seoses maksepettusega). Siinkohal võib olla oluline see, kas andmesubjekt või kolmandad isikud on asjaomased andmed juba avalikustanud. Asjaolu, et isikuandmed on avalikult kättesaadavad, võidaks arvesse võtta selle hindamisel, kas andmeid loodeti kasutada veel teatavatel konkreetsetel eesmärkidel. See kriteerium võib hõlmata ka isiklike dokumente, e-kirju, päevikuid, märkmete tegemist võimaldavaid e-lugereid ja väga isiklikku teavet, mis leidub kasutaja tegevust käsitlevaid andmeid registreerivates rakendustes (lifelogging).
5. Isikuandmete ulatuslik töötlemine: isikuandmete kaitse üldmääruses ei ole määratletud, mida tähendab ulatuslik, ehkki põhjenduses 91 on antud mõned juhised. Artikli 29 töörühm igal juhul soovib võtta selle kindlaks määramisel, kas isikuandmete töötlemine on ulatuslik, arvesse eeskätt järgmisi tegureid¹⁶:
 - a. asjaomaste andmesubjektide arv või osakaal asjaomases populatsioonis;
 - b. töödeldavate isikuandmete maht ja/või ulatus;
 - c. isikuandmete töötlemise kestus või pidevus;
 - d. isikuandmete töötlemise geograafiline ulatus.
6. Andmekogumite sobitamine või kombineerimine näiteks andmete puhul, mis saadakse kahe või enama isikuandmete töötlemise toiminguga, millel on erinev eesmärk ja/või mida teevad erinevad vastutavad töötlejad viisil, mis ületaks andmesubjekti põhjendatud ootusi¹⁷.
7. Haavatavate andmesubjektide andmed (põhjendus 75): seda liiki isikuandmete töötlemine on arvatud kriteeriumide hulka, sest andmesubjektide ja vastutava töötleja jõuvahekord on siin

¹⁵ Artikli 29 töörühma tõlgenduses tähendab „süstemaatiline“ vähemalt üht järgmistest (vt artikli 29 töörühma suunised andmekaitseametnike kohta (16/EN WP 243)):

- toimub vastavalt süsteemile;
- ettevalmistatud, korraldatud või meetodiline;
- on üldise andmete kogumise kava osa;
- on strateegia osa.

Artikli 29 töörühma tõlgenduse kohaselt on „avalik ala“ mis tahes koht, mis on avatud igale üldsuse esindajale, näiteks linnaväljak, ostukeskus, tänav, turuplats, rongijaam või avalik raamatukogu.

¹⁶ Vt artikli 29 töörühma suunised andmekaitseametnike kohta (16/EN WP 243).

¹⁷ Vt selgitus artikli 29 töörühma eesmärgi piirangut käsitleva arvamus (13/EN WP 203) leheküljel 24.

rohkem paigast ära, mis tähendab seda, et üksikisikutel ei pruugi olla lihtne nõustuda oma isikuandmete töötlemisega, olla sellele vastu või kasutada oma õigusi. Haavatavate andmesubjektide hulka võivad kuuluda lapsed (kelle puhul võidakse leida, et nad ei suuda teadlikult ja läbimõeldult olla vastu oma isikuandmete töötlemisele või sellega nõustuda), töötajad, erilist kaitset vajavad haavatavamad elanikkonnarühmad (vaimselt haiged inimesed, varjupaigataotlejad, eakad, patsiendid jne) ning igal juhul isikud, kelle puhul on võimalik kindlaks teha, et andmesubjekti ja vastutava töötleja jõuvahekord ei ole tasakaalus.

8. Uuenduslik kasutamine või uute tehnoloogiliste või korralduslike lahenduste rakendamine, nagu sõrmejälje ja näotuvastuse samaaegne kasutamine füüsilise juurdepääsukontrolli tõhustamiseks. Isikuandmete kaitse üldmääruses on selgelt öeldud (artikli 35 lõige 1 ning põhjendused 89 ja 91), et uue tehnoloogia kasutamisel „vastavalt tehnoloogiliste teadmiste tasemele“ (põhjendus 91) võib tekkida vajadus teha andmekaitsealane mõjuhindang. Seda põhjusel, et sellise tehnoloogia kasutamine võib hõlmata uudseid isikuandmete kogumise ja kasutamise viise, millega võib kaasneda suur oht üksikisikute õigustele ja vabadustele. Uue tehnoloogia kasutuselevõtu isiklikud ja sotsiaalsed tagajärjed ei pruugi olla tõepoolest teada. Andmekaitsealane mõjuhindang aitab vastutaval töötlejal selliseid ohte mõista ja käsitleda. Näiteks võib teatavatel asjade interneti rakendustel olla märkimisväärne mõju üksikisikute igapäevaelule ja eraelu puutumatusele ning seetõttu on nende puhul vaja teha andmekaitsealane mõjuhindang.
9. Kui isikuandmete töötlemise toimingud ise „takistavad andmesubjektidel õiguse või teenuse või lepingu kasutamist“ (artikkel 22 ja põhjendus 91). See hõlmab isikuandmete töötlemise toiminguid, mille eesmärk on võimaldada või kohandada juurdepääsu teenusele või lepingu sõlmimist või jätta andmesubjekt sellest võimalusest ilma. Selle näiteks on olukord, kus pank kontrollib oma kliente krediidiinfo andmebaasi alusel, et otsustada, kas anda klientidele laenu.

Enamikul juhtudel võib vastutav töötleja leida, et selliseks isikuandmete töötlemiseks, mille puhul on täidetud kaks kriteeriumi, oleks vaja teha andmekaitsealane mõjuhindang. Üldiselt on artikli 29 töörihm seda meelt, et mida rohkem kriteeriumeid on isikuandmete töötlemise puhul täidetud, seda suurema tõenäosusega kujutab see endast suurt ohtu andmesubjektide õigustele ja vabadustele ning seepärast eeldab see andmekaitsealast mõjuhindangut, olenemata meetmetest, mille vastutav töötleja kavatses võtta.

Mõnel juhul võib vastutav töötleja siiski leida, et andmekaitsealast mõjuhindangut on vaja ka vaid ühele kriteeriumile vastava isikuandmete töötlemise puhul.

Järgmiste näidete põhjal on näha, kuidas tuleks kõnealuseid kriteeriumeid kasutada, et hinnata, kas konkreetse isikuandmete töötlemise toimingu puhul on vaja andmekaitsealast mõjuhindangut.

Isikuandmete töötlemise näide	Võimalikud asjakohased kriteeriumid	Kas andmekaitsealane mõjuhindang on tõenäoliselt nõutav?
Haigla töötleb (haigla infosüsteemis) oma patsientide geneetilisi ja terviseandmeid.	<ul style="list-style-type: none"> - <u>Tundlikud andmed või väga isiklikud andmed</u> - Haavatavate andmesubjektide andmed - Isikuandmete ulatuslik töötlemine 	Jah

Isikuandmete töötlemise näide	Võimalikud asjakohased kriteeriumid	Kas andmekaitsealane mõjuhinna on tõenäoliselt nõutav?
Kaamerasüsteemi kasutamine, et jälgida sõidukijuhtide käitumist maanteel. Vastutav töötleja kavatseb kasutada arukat videoanalüüsi süsteemi, et eristada autod ja automaatselt tuvastada registreerimismärgid.	<ul style="list-style-type: none"> - Süstemaatiline jälgimine - Uuenduslik kasutamine või uute tehnoloogiliste või korralduslike lahenduste rakendamine 	
Ettevõtja jälgib süstemaatiliselt oma töötajate tegevust, sealhulgas kontrollib töötajate töökohta, interneti kasutamist jne.	<ul style="list-style-type: none"> - Süstemaatiline jälgimine - Haavatavate andmesubjektide andmed 	
Sotsiaalmeedias leiduvate avalike andmete kogumine profiilide loomiseks.	<ul style="list-style-type: none"> - Hindamine - Isikuandmete ulatuslik töötlemine - Andmekogumite sobitamine või kombineerimine - <u>Tundlikud andmed või väga isiklikud andmed</u> 	
Asutus loob riigi tasandil krediidireitingu või pettusevastase võitluse andmebaasi.	<ul style="list-style-type: none"> - Hindamine - Õiguslike või samaväärsete oluliste tagajärgedega automatiseeritud otsuste tegemine - Takistab andmesubjektil õiguse või teenuse või lepingu kasutamist - <u>Tundlikud andmed või väga isiklikud andmed</u> 	
Teadusprojektide või kliiniliste katsetega hõlmatud haavatavate andmesubjektide pseudonüümitud tundlike isikuandmete arhiveerimine.	<ul style="list-style-type: none"> - Tundlikud andmed - Haavatavate andmesubjektide andmed - Takistab andmesubjektil õiguse või teenuse või lepingu kasutamist 	
Patsientide või klientide isikuandmete töötlemine üksiku arsti, muu tervishoiutöötaja või juristi poolt (põhjendus 91).	<ul style="list-style-type: none"> - <u>Tundlikud andmed või väga isiklikud andmed</u> - Haavatavate andmesubjektide andmed 	Ei
Veebiajakiri kasutab meililisti, et saata oma tellijatele igapäevaseid üldiseid ülevaateid.	<ul style="list-style-type: none"> - Isikuandmete ulatuslik töötlemine 	
Vanasõidukite varuosi reklaamiv e-kaubanduse veebisait kasutab piiratud määral profiilanalüüsi, tuginedes teabele oma veebisaidil vaadatud või sealt ostetud varuosade kohta.	<ul style="list-style-type: none"> - Hindamine 	

Samas võib isikuandmete töötlemise toiming vastata mõnele eespool nimetatud juhtumile ja olla vastutava töötleja silmis ikkagi toiming, mille tulemusena ei teki tõenäoliselt suur ohtu. Sellistel juhtudel peaks vastutav töötleja esitama ja dokumenteerima põhjused, miks ta ei teinud andmekaitsealast mõjuhinna, ja lisama/registreerima andmekaitseametniku seisukoha.

Lisaks, kooskõlas vastutuse põhimõttega „registreerib [iga vastutav töötleja] tema vastutusel tehtavad isikuandmete töötlemise toimingud“, sealhulgas esitab järgmise teabe: töötlemise eesmärgid, andmesubjektide kategooriate ja isikuandmete liikide kirjeldus ning „võimaluse korral artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus“ (artikli 30 lõige 1). Samuti peab iga vastutav töötleja hindama, kas suur oht on tõenäoline, isegi kui ta lõppkokkuvõttes ei otsusta teha andmekaitsealast mõjuhinnaangut.

Märkus: järelevalveasutused peavad koostama ja avalikustama loetelu isikuandmete töötlemise toimingutest, mille puhul tuleb teha andmekaitsealane mõjuhinnaang, ning edastama selle loetelu Euroopa Andmekaitsekoostöökoostööle (artikli 35 lõige 4)¹⁸. Kõnealuse loetelu koostamisel võivad järelevalveasutustele abiks olla eespool sätestatud kriteeriumid. Vajaduse korral võidakse seda loetelu hiljem täpsustada. Näiteks võidakse artikli 35 lõike 4 kohase loetelu koostamisel pidada asjakohaseks ka mis tahes liiki biomeetriliste andmete või laste isikuandmete töötlemist.

- b) Millal ei nõuta andmekaitsealast mõjuhinnaangut? Siis, kui isikuandmete töötlemise tulemusena ei teki tõenäoliselt suurt ohtu, kui sarnane andmekaitsealane mõjuhinnaang on juba olemas, kui isikuandmete töötlemiseks on antud luba enne 2018. aasta maid, kui isikuandmete töötlemisel on õiguslik alus või kui isikuandmete töötlemine on nende töötlemistoimingute loetelus, mille puhul andmekaitsealast mõjuhinnaangut ei nõuta.

Artikli 29 töörihm leiab, et andmekaitsealast mõjuhinnaangut ei ole vaja järgmistel juhtudel:

- **kui isikuandmete töötlemise tulemusena tõenäoliselt ei teki füüsiliste isikute õigustele ja vabadustele suurt ohtu** (artikli 35 lõige 1);
- **kui isikuandmete töötlemine sarnaneb laadi, ulatuse, konteksti ja eesmärkide poolest suurel määral sellisele isikuandmete töötlemisele, millega seoses on andmekaitsealane mõjuhinnaang juba tehtud.** Sellisel juhul võib kasutada sarnase isikuandmete töötlemise jaoks koostatud andmekaitsealase mõjuhinnaangu tulemusi (artikli 35 lõige 1¹⁹);
- kui järelevalveasutus on kontrollinud isikuandmete töötlemise toiminguid enne 2018. aasta maid konkreetsetel tingimustel, mis ei ole muutunud²⁰ (vt III jaotise punkt C);
- **kui artikli 6 lõike 1 punkti c või e kohasel isikuandmete töötlemise toimingul on õiguslik alus**, mis tuleneb liidu või liikmesriigi õigusest, ja selle õigusega reguleeritakse konkreetset isikuandmete töötlemise toimingut **ja kui andmekaitsealane mõjuhinnaang on** kõnealuse õigusliku aluse vastuvõtmise raames **juba tehtud** (artikli 35 lõige 10),²¹ välja arvatud juhul, kui liikmesriigi kinnitusele on vaja teha enne töötlemist andmekaitsealane mõjuhinnaang;

¹⁸ Sellega seoses „kohaldab pädev järelevalveasutus artiklis 63 osutatud järjepidevuse mehhanismi, kui need loetelud hõlmavad isikuandmete töötlemise toiminguid, mis on seotud kaupade või teenuste pakkumisega andmesubjektidele või andmesubjektide käitumise jälgimisega mitmes liikmesriigis, või kui isikuandmete töötlemise toimingud võivad oluliselt mõjutada isikuandmete vaba liikumist liidus“ (artikli 35 lõige 6).

¹⁹ „Endast sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata koos.“

²⁰ „Direktiivi 95/46/EÜ alusel komisjoni vastu võetud otsused ja järelevalveasutuste antud load jäävad kehtima nende muutmise, asendamise või kehtetuks tunnistamiseni“ (põhjendus 171).

²¹ Kui andmekaitsealane mõjuhinnaang on koostatud isikuandmete töötlemisele õigusliku aluse tagava õigusakti väljatöötamise etapis, tuleb see tõenäoliselt enne isikuandmete töötlemisega alustamist läbi vaadata, sest vastuvõetud õigusakt võib erineda õigusakti vastuvõtmise ettepanekust viisil, mis mõjutab eraelu puutumatuse ja isikuandmete kaitset seotud küsimusi. Pealegi, isegi kui andmekaitsealane mõjuhinnaang tehti, ei pruukinud õigusakti vastuvõtmise ajal olla tegelikult isikuandmete töötlemise kohta olemas piisavalt palju tehnilisi üksikasju. Sellisel juhul võib enne isikuandmete töötlemise toimingute tegelikku tegemist ikkagi olla vajalik koostada eraldi andmekaitsealane mõjuhinnaang.

- **kui isikuandmete töötlemise toiming on kantud (järelevalveasutuse poolt) vabatahtlikult koostatavasse loetellu, mis sisaldab selliseid isikuandmete töötlemise toiminguid, mille puhul andmekaitsealast mõjuhinna eest ei nõuta (artikli 35 lõige 5).** Selline loetelu võib hõlmata isikuandmete töötlemise toiminguid, mis vastavad tingimustele, mille asjaomane järelevalveasutus on kindlaks määranud eelkõige suunistes, konkreetsetes otsustes või lubades, vastavuseeskirjades jm (nt Prantsusmaal load, erandid, lihtsustatud eeskirjad, vastavuspaketid jne). Sellisel juhul ei ole tingimusel, et pädev järelevalveasutus teeb kordushindamise, andmekaitsealast mõjuhinna eest vaja, ent üksnes siis, kui isikuandmete töötlemine jääb rangelt loetelus nimetud isikuandmete töötlemise piiresse ja on endiselt täielikult kooskõlas isikuandmete kaitse üldmääruse asjakohaste nõuetega.

C. Kuidas on lood juba käsil olevate isikuandmete töötlemise toimingutega? Teatavatel asjaoludel on nõutav andmekaitsealane mõjuhinna eest.

Nõue teha andmekaitsealane mõjuhinna eest kehtib nende juba käsil olevate isikuandmete töötlemise toimingute puhul, mille tulemusena tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht ning millega kaasnevad ohud on muutunud, võttes arvesse isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke.

Andmekaitsealast mõjuhinna eest ei ole vaja isikuandmete töötlemise toimingute puhul, mida järelevalveasutus või andmekaitseametnik on kontrollinud kooskõlas direktiivi 95/46/EÜ artikliga 20 ja mida tehakse viisil, mis ei ole pärast eelnevat kontrolli muutunud. Tõepoolest, „[d]irektiivi 95/46/EÜ alusel komisjoni vastu võetud otsused ja järelevalveasutuste antud load jäävad kehtima nende muutmise, asendamise või kehtetuks tunnistamiseni“ (põhjendus 171).

Seevastu iga isikuandmete töötlemise toimingu puhul, mille tegemise tingimused (ulatus, eesmärk, kogutavad isikuandmed, vastutava töötleja või isikuandmete vastuvõtja isik, isikuandmete säilitamise tähtaeg, tehnilised ja korralduslikud meetmed jne) on pärast järelevalveasutuse või andmekaitseametniku tehtud eelnevat kontrolli muutunud ning mille tulemusena tõenäoliselt tekib suur oht, tuleks teha andmekaitsealane mõjuhinna eest.

Lisaks võidakse andmekaitsealast mõjuhinna eest nõuda siis, kui isikuandmete töötlemise toimingutest tulenevad ohud on muutunud,²² näiteks uue tehnoloogia kasutuselevõtu tõttu või seoses sellega, et isikuandmeid kasutatakse muul eesmärgil. Isikuandmete töötlemise toimingud võivad areneda kiiresti ja esile võivad kerkida uued nõrgad kohad. Seepärast tuleb märkida, et andmekaitsealase mõjuhinna läbivaatamine on – peale selle, et see on kasulik pidevaks täiustuste tegemiseks – ülioluline, et säilitada aja jooksul muutuv keskkonnas andmekaitse tase. Andmekaitsealane mõjuhinna eest võib muutuda vajalikuks ka isikuandmete töötlemise korraldusliku või sotsiaalse konteksti muutumisel, näiteks kui on suurenenud teatavate automatiseeritud otsuste mõju või kui diskrimineerimise suhtes on muutunud haavatavaks uued andmesubjektide kategooriad. Kõik need näited võivad kaasa tuua asjaomase isikuandmete töötlemise toimingu tulemusel tekkiva ohu muutumise.

Samas võivad teatavad muudatused ka ohtu vähendada. Näiteks võib isikuandmete töötlemise toiming areneda nii, et otsused ei ole enam automatiseeritud või jälgimine ei ole enam süstemaatiline. Sellisel

²² Muutunud on kontekst, kogutavad isikuandmed, eesmärgid, funktsionaalsus, töödeldavad isikuandmed, isikuandmete vastuvõtjad, isikuandmete kombinatsioonid, ohud (toetavad varad, ohuallikad, võimalik mõju jne), turvameetmed ja isikuandmete rahvusvaheline edastamine.

juhul võib tehtud riskianalüüsi läbivaatamisel ilmned, et andmekaitsealase mõjuhinna koostamine ei ole enam vajalik.

Hea tava kohaselt **tuleks andmekaitsealane mõjuhinna pidevalt läbi vaadata ja seda tuleks korrapäraselt uuesti hinnata**. Seepärast on ka juhul, kui 25. mail 2018 andmekaitsealast mõjuhinna ei nõuta, vajalik, et vastutav töötleja koostaks selle asjakohasel ajal oma üldiste vastutusega seotud kohustuste täitmise raames.

D. Kuidas teha andmekaitsealane mõjuhinna?

a) Millal tuleks andmekaitsealane mõjuhinna teha? Enne isikuandmete töötlemist.

Andmekaitsealane mõjuhinna tuleks teha „enne isikuandmete töötlemist“ (artikli 35 lõiked 1 ja 10 ning põhjendused 90 ja 93)²³. See on kooskõlas lõimitud andmekaitse ja vaikimisi andmekaitse põhimõttega (artikkel 25 ja põhjendus 78). Andmekaitsealases mõjuhinna koostamisel tuleks näha vahendit, mis aitab teha isikuandmete töötlemisega seotud otsuseid.

Andmekaitsealast mõjuhinna koostama hakata koostama isikuandmete töötlemise kavandamisel võimalikult vara, isegi kui mõni isikuandmete töötlemise toiming ei ole veel teada. Andmekaitsealase mõjuhinna ajakohastamisega projekti elluviimise vältel tagatakse isikuandmete kaitse ja eraelu puutumatuse arvessevõtmine ning toetatakse vastavust edendatavate lahenduste väljatöötamist. Isikuandmete töötlemise kavandamise edenedes võib tekkida vajadus korrata hindamise üksikuid etappe, sest teatavate tehniliste või korralduslike meetmete valik võib mõjutada isikuandmete töötlemisega kaasnevate ohtude suurust või tõenäosust.

Asjaolu, et pärast isikuandmete töötlemisega alustamist võib osutuda vajalikuks andmekaitsealast mõjuhinna koostamist ajakohastada, ei ole mõjuv põhjus jätta andmekaitsealane mõjuhinna tegemata. Andmekaitsealase mõjuhinna koostamine on kestev protsess, eriti kui isikuandmete töötlemine on dünaamiline ja muutub pidevalt. **Andmekaitsealase mõjuhinna tegemine on pidev protsess, mitte ühekordne ülesanne.**

b) Kes on kohustatud tegema andmekaitsealase mõjuhinna? Vastutav töötleja koos andmekaitseametniku ja volitatud töötlejatega.

Andmekaitsealase mõjuhinna tegemise eest vastutab vastutav töötleja (artikli 35 lõige 2). Mõjuhinna võib koostada keegi teine organisatsiooni sees või sellest väljaspool, kuid vastutus selle ülesande täitmise eest lasub täielikult vastutaval töötlejal.

Vastutav töötleja peab küsima ka nõu andmekaitseametnikult, kui viimane on määratud (artikli 35 lõige 2), ning antud nõu ja vastutava töötleja otsused tuleks dokumenteerida andmekaitsealases mõjuhinna koostamisel. Andmekaitseametnik peaks ka jälgima andmekaitsealase mõjuhinna toimimist (artikli 39 lõike 1 punkt c). Lisajuhised on esitatud artikli 29 tööriista suunistes andmekaitseametnike kohta (16/EN WP 243).

²³ Välja on arvatud juhud, mil tegemist on juba toimuva isikuandmete töötlemisega, mida järelevalveasutus on eelnevalt kontrollinud. Sellistel juhtudel tuleks andmekaitsealane mõjuhinna koostada enne oluliste muudatuste tegemist.

Kui isikuandmeid töötleb täies ulatuses või osaliselt volitatud töötleja, **peaks volitatud töötleja vastutavat töötlejat andmekaitsealase mõjuhinna tegemisel abistama** ja esitama mis tahes vajaliku teabe (kooskõlas artikli 28 lõike 3 punktiga f).

„Vajaduse korral“ peab vastutav töötleja küsima **„andmesubjektide või nende esindajate seisukohti“** (artikli 35 lõige 9). Artikli 29 töörihm leiab, et

- nende seisukohtade küsimiseks saab kasutada sõltuvalt kontekstist eri vahendeid (nt üldine uuring isikuandmete töötlemise toimingute eesmärgi ja vahendite kohta, küsimus töötajate esindajatele või tavaline küsimustik, mis saadetakse vastutava töötleja tulevastele klientidele); hoolt tuleb kanda selle eest, et vastutaval töötlejal on selliste seisukohtade küsimisega kaasnevaks mis tahes isikuandmete töötlemiseks seaduslik alus. Tuleb siiski märkida, et isikuandmete töötlemiseks nõusoleku hankimine ei ole ilmselgelt viis, kuidas küsida andmesubjektide seisukohti;
- kui vastutava töötleja lõplik otsus erineb andmesubjektide seisukohtadest, tuleks dokumenteerida jätkamise või mittejätkamise põhjused;
- samuti peaks vastutav töötleja dokumenteerima põhjenduse sellele, miks ta ei küsi andmesubjektide seisukohti, kui ta otsustab, et see ei ole asjakohane (näiteks kui see kahjustaks ettevõtjate äriplaanide konfidentsiaalsust) või et see on ebaproportsionaalne või võimatu.

Lõpetuseks on hea tava määrata kindlaks ja dokumenteerida muud sisepoliitikast, -protsessidest ja -eeskirjadest sõltuvad konkreetsed rollid ja ülesanded, näiteks:

- kui konkreetsed äriüksused võivad esitada ettepaneku teha andmekaitsealane mõjuhinna, peaksid need üksused andma sellesse oma panuse ja nad tuleks kaasata mõjuhinna kinnitamise protsessi;
- kui see on asjakohane, soovitatakse küsida nõu eri kutsealade sõltumatutelt ekspertidelt²⁴ (juristid, IT-eksperdid, turvaekspertid, sotsioloogid, eetikaekspertid jne);
- volitatud töötlejate rollid ja ülesanded peavad olema lepingus kindlaks määratud; andmekaitsealane mõjuhinna tuleb teha volitatud töötleja abiga, võttes arvesse isikuandmete töötlemise laadi ja volitatud töötlejale kättesaadavat teavet (artikli 28 lõike 3 punkt f);
- infoturbe juht, kui see on määratud, ja andmekaitseametnik võiksid soovitada vastutaval töötlejal teha konkreetse isikuandmete töötlemise toimingute puhul andmekaitsealane mõjuhinna ning peaksid aitama sidusrühmi seoses meetodikaga, samuti peaksid nad aitama hinnata riskihindamise kvaliteeti ja seda, kas jääkrisk on vastuvõetav, ning aitama suurendada vastutava töötleja tegevusega seotud eriteadmisi;
- infoturbe juht, kui see on määratud, ja/või IT-osakond peaksid pakkuma vastutavale töötlejale abi ning võiksid teha ettepaneku koostada konkreetse isikuandmete töötlemise toimingute puhul andmekaitsealane mõjuhinna, sõltuvalt turvalisuse või tegevusega seotud vajadustest.

- c) Millist meetodikat tuleks rakendada andmekaitsealase mõjuhinna tegemisel?
Meetodikad on erinevad, kuid kriteeriumid on ühised.

²⁴ *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3*, http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Isikuandmete kaitse üldmääruses on sätestatud andmekaitsealase mõjuhinna miinimumsisu (artikli 35 lõige 7 ning põhjendused 84 ja 90):

- „kavandatud isikuandmete töötlemise toimingute ja töötlemise eesmärkide [---] kirjeldus“;
- „isikuandmete töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine“;
- „andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnang“;
- „kavandatud meetmed“
 - o „ohtude käsitlemiseks“;
 - o „määruse järgimise tõendamiseks“.

Järgneval joonisel on kajastatud üldist korduvat andmekaitsealase mõjuhinna tegemise protsessi²⁵.



Isikuandmete töötlemise toimingu mõju hindamisel tuleb arvesse võtta toimimisjuhendi järgimist (artikkel 40 ja artikli 35 lõige 8). See võib olla kasulik selle tõendamisel, et valitud või kehtestatud on piisavad meetmed, tingimusel et toimimisjuhend on asjaomase isikuandmete töötlemise toimingu puhul asjakohane. Samuti tuleks arvesse võtta sertifikaate, pitsereid ja märgiseid (artikkel 42), mille eesmärk on tõendada vastutavate töötlejate ja volitatud töötlejate teostatavate isikuandmete töötlemise toimingute vastavust isikuandmete kaitse üldmäärusele, ning siduvaid kontsernisisesid eeskirju.

Kõik isikuandmete kaitse üldmääruses sätestatud asjakohased nõuded tagavad ulatusliku üldise raamistiku andmekaitsealase mõjuhinna kavandamiseks ja tegemiseks. Andmekaitsealase mõjuhinna rakendamine praktikas sõltub isikuandmete kaitse üldmääruses sätestatud nõuetest, mida võidakse täiendada üksikasjalikumate praktiliste juhistega. Seega on andmekaitsealase mõjuhinna rakendamine kohandatav. See tähendab, et isegi väike vastutav töötleja saab koostada

²⁵ Tuleks rõhutada, et joonisel kirjeldatud protsess on korduv: praktikas on tõenäoline, et iga etapp läbitakse enne andmekaitsealase mõjuhinna valmimist mitu korda.

andmekaitsealase mõjuhinnangu, mis sobib tema isikuandmete töötlemise toimingute jaoks, ja seda rakendada.

Isikuandmete kaitse üldmääruse põhjenduses 90 on loetletud hulk andmekaitsealase mõjuhinnangu elemente, mis kattuvad riskijuhtimise täpselt määratletud elementidega (nt ISO 31000²⁶). Riskijuhtimise vaatenurgast on andmekaitsealase mõjuhinnangu eesmärk tegeleda füüsiliste isikute õigusi ja vabadusi ähvardavate ohtudega,

- määrates kindlaks konteksti, „*võttes arvesse töötlemise laadi, ulatust, konteksti ja eesmärke ning ohu allikaid*“;
- hinnates ohte „*suure ohu konkreetse tõenäosuse ja tõsiduse hindamiseks*“;
- käsitledes ohte „*selle ohu leevendamiseks*“, „*isikuandmete kaitse tagamiseks*“ ja „*määruse täitmise tõendamiseks*“.

Märkus: isikuandmete kaitse üldmääruse kohane andmekaitsealane mõjuhinnang on vahend, mille abil käsitletakse andmesubjektide õigusi ja vabadusi ähvardavaid ohte, seega lähtutakse selles teatavate valdkondade puhul (nt ühiskondlik julgeolek) andmesubjektide vaatenurgast. Riskijuhtimisel muudes valdkondades (nt infoturve) keskendutakse seevastu organisatsioonile.

Isikuandmete kaitse üldmäärus võimaldab vastutavatel töötajatel olla andmekaitsealase mõjuhinnangu täpse ülesehituse ja vormi kindlaksmääramisel paindlik, et seda hinnangut saaks koostada kooskõlas olemasolevate töötavadega. ELis ja kogu maailmas on sisse seatud suur hulk erinevaid protsesse, milles võetakse arvesse põhjenduses 90 kirjeldatud elemente. Olenemata sellest, milline on andmekaitsealase mõjuhinnangu vorm, tuleb selles siiski tõeliselt hinnata ohte, et vastutavad töötajad saaksid võtta nende kõrvaldamiseks meetmeid.

Isikuandmete kaitse üldmääruses sätestatud põhinõuete täitmisel võib kasutada eri metoodikaid (vt 1. lisas esitatud näited andmekaitse ja eraelu puutumatuse alase mõju hindamise metoodikate kohta). Et võimaldada neil erinevatel lähenemisviisidel kõrvuti eksisteerida ja samal ajal võimaldada vastutavatel töötajatel järgida isikuandmete kaitse üldmäärust, on kindlaks määratud ühised kriteeriumid (vt 2. lisa). Neis selgitatakse määruse põhinõudeid, ent jäetakse piisavalt võimalusi eri rakendamisviiside jaoks. Kõnealuseid kriteeriume saab kasutada selle tõendamiseks, et andmekaitsealase mõjuhinnangu koostamisel kasutatud konkreetne metoodika on kooskõlas standarditega, mille järgimist isikuandmete kaitse üldmääruses nõutakse. **Vastutav töötaja võib valida ise metoodika, kuid see metoodika peaks vastama 2. lisas esitatud kriteeriumidele.**

Artikli 29 töörihm toetab andmekaitsealase mõju hindamise valdkonnapõhiste raamistike väljatöötamist. Seda põhjusel, et neis saab tugineda konkreetsetele valdkondlikele teadmistele, tänu millele saab andmekaitsealases mõjuhinnangus käsitleda teatavat liiki töötlemistoimingute eripärasid (nt konkreetset liiki andmed, äriühingu varad, võimalik mõju, ohud, meetmed). See tähendab, et andmekaitsealases mõjuhinnangus saab käsitleda küsimusi, mis tekivad konkreetsetes majandusvaldkonnas, konkreetse tehnoloogia kasutamisel või konkreetset liiki töötlemistoimingute tegemisel.

²⁶ Riskijuhtimisprotsessid: teabevahetus ja konsulteerimine, konteksti kindlaksmääramine, riskide hindamine, riskide käsitlemine, jälgimine ja läbivaatamine (vt standardit ISO 31000 käsitleva ülevaate (<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>) punkt „Terms and definitions“).

Lõpetuseks lisame, et „[v]astutav töötleja hindab asjakohasel juhul ja vähemalt isikuandmete töötlemise toimingutest tuleneva ohu muutumise korral, kas isikuandmete töötlemine vastab andmekaitsealasele mõjuhinnaangule“ (artikli 35 lõige 11²⁷).

- d) Kas on olemas kohustus andmekaitsealane mõjuhinnaang avaldada? Ei, kuid kokkuvõtte avaldamine võib suurendada usaldust ning eelneva konsulteerimise või andmekaitseasutuse taotluse korral tuleb andmekaitsealane mõjuhinnaang tervikuna edastada järelevalveasutusele.

Andmekaitsealase mõjuhinnaangu avaldamine ei ole isikuandmete kaitse üldmäärusest tulenev õiguslik nõue, vaid vastutava töötleja otsus seda teha. Vastutavad töötlejad peaksid siiski kaaluma vähemalt andmekaitsealase mõjuhinnaangu osade, näiteks kokkuvõtte või järelduste avaldamist.

Selle eesmärk on suurendada usaldust vastutava töötleja isikuandmete töötlemise toimingute suhtes ning tõendada vastutust ja läbipaistvust. Eriti hea tava on avaldada andmekaitsealane mõjuhinnaang juhul, kui isikuandmete töötlemise toiming mõjutab üldsuse esindajaid. Nii võib see olla eeskätt siis, kui andmekaitsealase mõjuhinnaangu koostab avaliku sektori asutus.

Andmekaitsealase mõjuhinnaangu avaldamisel ei tule avaldada kogu hinnaang, eriti kui see võib sisaldada konkreetset teavet vastutava töötleja turvariskide kohta või paljastada ärisaladusi või äriliselt tundlikku teavet. Taolistel asjaoludel võib avaldatud versioon koosneda lihtsalt andmekaitsealase mõjuhinnaangu põhijärelduste kokkuvõttest või isegi lihtsalt kinnitusest, et andmekaitsealane mõjuhinnaang on tehtud.

Peale selle, kui andmekaitsealasest mõjuhinnaangust ilmnevad suured jääkriskid, peab vastutav töötleja konsulteerima enne isikuandmete töötlemist järelevalveasutusega (artikli 36 lõige 1). Selle raames tuleb esitada täielik andmekaitsealane mõjuhinnaang (artikli 36 lõike 3 punkt e). Järelevalveasutus võib anda nõu,²⁸ paljastamata ärisaladusi või turvalisusega seotud nõrku kohti, kooskõlas põhimõtetega, mida kohaldatakse liikmesriigis seoses avaliku juurdepääsuga ametlikele dokumendile.

E. Millal tuleks konsulteerida järelevalveasutusega? Siis, kui jääkriskid on suured.

Nagu on selgitatud eespool,

- nõutakse andmekaitsealast mõjuhinnaangut juhul, kui isikuandmete töötlemise toimingu tulemusena „tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht“ (artikli 35 lõige 1, vt III jaotise punkti B alapunkt a). Isikuandmete töötlemise toiminguks, mille tulemusena tekib tõenäoliselt suur oht ja mille puhul on vaja teha andmekaitsealane mõjuhinnaang, peetakse näiteks terviseandmete ulatuslikku töötlemist;
- vastutaval töötlejal tuleb hinnata andmesubjektide õigusi ja vabadusi ähvardavaid ohte, teha kindlaks meetmed,²⁹ mille abil vähendatakse neid ohte vastuvõetava tasemeni, ja tõendada määruse järgimist (artikli 35 lõige 7, vt III jaotise punkti C alapunkt c). Näitena võib tuua asjakohaste tehniliste ja korralduslike turvameetmete kasutamise (kogu ketta tõhus

²⁷ Artikli 35 lõikes 10 on sõnaselgelt sätestatud erand vaid artikli 35 lõigete 1–7 kohaldamisest.

²⁸ Kirjalikku nõu tuleb anda vastutavale töötlejale vaid juhul, kui järelevalveasutus on seisukohal, et kavandatav isikuandmete töötlemine ei ole määrusega kooskõlas, nagu on sätestatud artikli 36 lõikes 2.

²⁹ Võttes muu hulgas arvesse Euroopa Andmekaitsekoogu ja järelevalveasutuste kehtivaid suuniseid, samuti teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid, nagu on ette nähtud artikli 35 lõikes 1.

krüpteerimine, võtmete usaldusväärne haldamine, asjakohane juurdepääsukontroll, turvaline varundamine jne) lisaks kehtivale poliitikale (teavitamine, nõusolek, õigus isikuandmetega tutvuda, õigus esitada vastuväiteid jne) isikuandmete säilitamise korral sülearvutites.

Kui eespool näitena esitatud sülearvutite juhtumi puhul leitakse, et vastutav töötleja on ohte piisavalt vähendanud, võib töötlemine pärast artikli 36 lõike 1 ning põhjenduste 84 ja 94 lugemist jätkuda järelevalveasutusega konsulteerimata. Vastutav töötleja peab konsulteerima järelevalveasutusega juhul, kui ta ei suuda kindlaks tehtud ohte piisavalt käsitleda (st jääkriskid on endiselt suured).

Vastuvõetamatult suur jääkrisk esineb näiteks juhul, kui andmesubjektidel tuleb silmitsi seista märkimisväärsete või isegi pöördumatute tagajärgedega, millega nad ei pruugi toime tulla (nt oht andmesubjektide elule, mis on põhjustatud ebaseaduslikust juurdepääsust isikuandmetele, koondamine, oht finantsstabiilsusele), ja/või kui on ilmne, et oht kordub (nt kuna isikuandmete jagamise, kasutamise või levitamise viisi tõttu ei ole võimalik vähendada isikuandmetele ligi pääsevate isikute arvu või kuna hästi teada nõrga kohaga ei ole tegeletud).

Kui vastutav töötleja ei leia piisavaid meetmeid, et vähendada ohud vastuvõetava tasemeni (st jääkriskid on endiselt suured), tuleb konsulteerida järelevalveasutusega³⁰.

Peale selle tuleb vastutaval töötlejal konsulteerida järelevalveasutusega, kui liikmesriigi õiguses nõutakse, et vastutavad töötlejad peavad konsulteerima järelevalveasutusega ja/või saada järelevalveasutuselt eelneva loa selleks, et töödelda isikuandmeid enda poolt avalikes huvides täidetava ülesande raames, sealhulgas töödelda isikuandmeid seoses sotsiaalkaitse ja rahvaterviseiga (artikli 36 lõige 5).

Tuleks siiski märkida, et olenemata sellest, kas jääkriski tasemest tulenevalt nõutakse või ei nõuta konsulteerimist järelevalveasutusega, säilib kohustus säilitada andmekaitsealane mõjuhindang ja seda õigel ajal ajakohastada.

IV. Järeldused ja soovitused

Andmekaitsealane mõjuhindang on vastutavatele töötlejatele kasulik vahend, et rakendada isikuandmete kaitse üldmäärusele vastavaid isikuandmete töötlemise süsteeme. Mõne isikuandmete töötlemise toimingu puhul võib andmekaitsealase mõjuhindangu koostamine olla kohustuslik. Kõnealused mõjuhindangud on kohandatavad ja need võib teha eri vormis, kuid isikuandmete kaitse üldmääruses on sätestatud tõhusa andmekaitsealase mõjuhindangu põhinõuded. Vastutavad töötlejad peaksid käsutama andmekaitsealase mõjuhindangu koostamist kasuliku ja positiivse tegevusena, mis aitab tagada vastavuse õigusnormidele.

Artikli 24 lõikes 1 on kindlaks määratud vastutava töötleja põhiülesanne isikuandmete kaitse üldmääruse järgimisel: „Arvestades töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte, rakendab vastutav töötleja asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete

³⁰ Märkus: „isikuandmete pseudonüümiseerimine ja krüpteerimine“ (nagu ka isikuandmete minimeerimine, järelevalvemehhanismid jne) ei ole ilmtingimata asjakohased meetmed. Need on vaid näited. Asjakohased meetmed sõltuvad isikuandmete töötlemise toimingute kontekstist ja kaasnevatest ohtudest.

töötlemist kooskõlas käesoleva määrusega. Vajaduse korral vaadatakse need meetmed läbi ja ajakohastatakse neid.“

Andmekaitsealasel mõjuhinnangul on määruse järgimisel väga oluline roll, juhul kui on kavas või toimub isikuandmete töötlemine, millega kaasneb suur oht. Vastutavad töötlejad peaksid kasutama käesolevas dokumendis esitatud kriteeriume, et teha kindlaks, kas on vaja koostada andmekaitsealane mõjuhinnang. Vastutava töötleja sisepoliitikas võib seda loetelu laiendada, minnes isikuandmete kaitse üldmääruks sätestatud õiguslikest nõuetest kaugemale. Selle tulemuseks peaks olema andmesubjektide ja teiste vastutavate töötlejate suurem usaldus ja kindlus.

Kavandades sellist isikuandmete töötlemist, mille tulemusena tekib tõenäoliselt suur oht, peab vastutav töötleja

- valima andmekaitsealase mõjuhinnangu tegemise metoodika (näited on esitatud 1. lisas), mis vastab 2. lisas esitatud kriteeriumidele, või määrama andmekaitsealase mõju hindamiseks kindlaks sellise süstemaatilise protsessi ja seda rakendama,
 - o mis vastab 2. lisas esitatud kriteeriumidele,
 - o mis on lõimitud kooskõlas sisemiste protsesside ning sisemise konteksti ja kultuuriga olemasolevatesse kavandamise, arendamise, muudatuste tegemise, riskide hindamise ja tegevuse läbivaatamise protsessidesse,
 - o millesse kaasatakse asjakohased huvitatud isikud (vastutav töötleja, andmekaitseametnik, andmesubjektid või nende esindajad, ettevõtjad, tehnilised talitused, volitatud töötlejad, infoturbe juht jne) ja määratakse selgelt kindlaks nende ülesanded;
- esitama pädevale järelevalveasutusele andmekaitsealase mõjuhinnangu aruande, kui tal palutakse seda teha;
- konsulteerima järelevalveasutusega, kui ta ei ole suutnud määrata suurte ohtude leevendamiseks kindlaks piisavaid meetmeid;
- vaatama korrapäraselt läbi andmekaitsealase mõjuhinnangu ja isikuandmete töötlemise toimingud, mida selles hinnatakse, või tegema seda vähemalt siis, kui isikuandmete töötlemisega kaasneb oht muutub;
- dokumenteerima tehtud otsused.

1. lisa. ELi andmekaitsealase mõju hindamise kehtivate raamistike näited

Isikuandmete kaitse üldmääruses ei ole sätestatud, millist andmekaitsealase mõju hindamise protsessi tuleks järgida. Selle asemel lubab määrus vastutavatel töötajatel kehtestada raamistiku, mis täiendab nende olemasolevaid töötavasid, tingimusel et selles on arvesse võetud artikli 35 lõikes 7 kirjeldatud elemente. Selline raamistik võib olla mõeldud konkreetse vastutava töötaja jaoks või võib olla kogu sektoril ühine. Allpool on esitatud mõned näited varem avaldatud ELi andmekaitseasutuste välja töötatud raamistike ja ELi valdkonnapõhiste raamistike kohta.

ELi üldised raamistikud:

- Saksamaa: Standard Data Protection Model, V.1.0 – Trial version, 2016³¹.
https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- Hispaania: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Prantsusmaa: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015
<https://www.cnil.fr/fr/node/15798>
- Ühendkuningriik: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

ELi valdkonnapõhised raamistikud:

- eraelu puutumatusele ja andmekaitsele avaldatava mõju hindamise raamistik RFID-rakenduste jaoks³²
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_et.pdf.
- arukate võrkude ja arukate arvestisüsteemide poolt andmekaitsele avaldatava mõju hindamise näidisvorm³³
http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Andmekaitsealase mõju hindamise metoodikaid käsitlevaid juhiseid antakse ka rahvusvahelises standardis (ISO/IEC 29134³⁴).

³¹ Raamistik kiideti ühehäälselt heaks (Baieri liidumaa jäi erapooletuks) 9.–10. novembril 2016 Kühlungsbornis toimunud föderaalsete ja liidumaade sõltumatute andmekaitseasutuste 92. konverentsil.

³² Vt ka:

- komisjoni 12. mai 2009. aasta soovitus eraelu puutumatuse ja andmekaitse põhimõtete kohaldamise kohta raadiosagedustuvastust kasutavates rakendustes,
<http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1508055265400&uri=CELEX:32009H0387;>
- arvamus 9/2011, mis käsitleb tööstusharu läbivaadatud ettepanekut RFID-rakenduste poolt eraelu puutumatusele ja andmekaitsele avaldatava mõju hindamise kohta,
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_et.pdf.

³³ Vt ka arvamus 07/2013, milles käsitletakse isikuandmete kaitsele avaldatava mõju hinnangu näidisvormi (edaspidi „näidisvorm“), mille on arukate võrkude ja arukate mõõtmissüsteemide jaoks koostanud komisjoni arukate võrkude töökonna 2. eksperidirühm. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_et.pdf.

2. lisa. Andmekaitsealase mõjuhinnangu kriteeriumid

Artikli 29 tööühm pakub välja järgmised kriteeriumid, mida vastutavad töötlejad saavad kasutada, et hinnata, kas andmekaitsealane mõjuhinnang või selle koostamise metoodika on piisavalt põhjalik, et olla kooskõlas isikuandmete kaitse üldmäärusega:

- ☐ esitatud on isikuandmete töötlemise süstemaatiline kirjeldus (artikli 35 lõike 7 punkt a):
 - ☐ arvesse on võetud isikuandmete töötlemise laadi, ulatust, konteksti ja eesmäärke (põhjendus 90),
 - ☐ registreeritud on isikuandmed, nende vastuvõtjad ja nende säilitamise tähtaeg,
 - ☐ esitatud on isikuandmete töötlemise toimingute funktsionaalne kirjeldus,
 - ☐ kindlaks on määratud vahendid (riistvara, tarkvara, võrgustikud, inimesed, paberkandjad või paberkandjate edastamise kanalid), millele isikuandmed tuginevad,
 - ☐ arvesse on võetud heakskiidetud toimumisjuhendi järgimist (artikli 35 lõige 8);
- ☐ hinnatud on vajalikkust ja proportsionaalsust (artikli 35 lõike 7 punkt b):
 - ☐ kindlaks on määratud meetmed, millega tagatakse määruse järgimine (artikli 35 lõike 7 punkt d ja põhjendus 90), sealhulgas
 - ☐ meetmed, mis aitavad tagada isikuandmete töötlemise proportsionaalsuse ja vajalikkuse, tuginedes järgmisele:
 - ☐ täpselt ja selgelt kindlaks määratud ning õiguspärased eesmärgid (artikli 5 lõike 1 punkt b),
 - ☐ isikuandmete töötlemise seaduslikkus (artikkel 6),
 - ☐ asjakohased, olulised ja vaid vajalikud andmed (artikli 5 lõike 1 punkt c),
 - ☐ säilitamise piiratud kestus (artikli 5 lõike 1 punkt e);
 - ☐ meetmed, mis aitavad kaitsta andmesubjektide õigusi, hõlmates järgmist:
 - ☐ andmesubjekti teavitamine (artiklid 12, 13 ja 14),
 - ☐ andmetega tutvumise ja andmete ülekandmise õigus (artiklid 15 ja 20),
 - ☐ õigus andmete parandamisele ja kustutamisele (artiklid 16, 17 ja 19),
 - ☐ õigus esitada vastuväiteid ja õigus isikuandmete töötlemise piiramisele (artiklid 18, 19 ja 21),
 - ☐ suhted volitatud töötlejatega (artikkel 28),
 - ☐ isikuandmete rahvusvahelise edastamisega seotud kaitsemeetmed (V peatükk),
 - ☐ eelnev konsulteerimine (artikkel 36);
- ☐ käsitletud on ohte andmesubjektide õigustele ja vabadustele (artikli 35 lõike 7 punkt c):
 - ☐ hinnatud on ohtude päritolu, laadi, eripära ja tõsidust (põhjendus 84) või iga ohu puhul (ebaseaduslik juurdepääs, soovimatu muutmine ja andmete kadumine) on andmesubjektide vaatenurgast
 - ☐ võetud arvesse ohtude allikaid (põhjendus 90),
 - ☐ tehtud kindlaks ebaseadusliku juurdepääsu, soovimatu muutmise ja andmete kadumise võimalik mõju andmesubjektide õigustele ja vabadustele,
 - ☐ tehtud kindlaks ohud, mis võivad kaasa tuua ebaseadusliku juurdepääsu, soovimatu muutmise ja andmete kadumise,
 - ☐ hinnatud tõenäosust ja tõsidust (põhjendus 90);
 - ☐ kindlaks on määratud meetmed, mille abil neid ohte käsitleda (artikli 35 lõike 7 punkt d ja põhjendus 90);
- ☐ kaasatud on huvitatud isikud:
 - ☐ küsitud on nõu andmekaitseametnikult (artikli 35 lõige 2),

³⁴ Rahvusvaheline Standardiorganisatsioon (ISO), ISO/IEC 29134 (projekt) – infotehnoloogia – turbetehnika – eraelu puutumatusele avalduva mõju hindamine – juhised.

- ☐ vajaduse korral on küsitud andmesubjektide või nende esindajate seisukohti (artikli 35 lõige 9).