Andmekaitse toote ja teenuse elutsüklis

Veebiseminar

14. veebruaril kell 9.30

SORAINEN

GDPRi A&O ehk nõuded, millest ei saa üle ega ümber

SORAINEN

Kirsi Koistinen
Tallinn

14 veebruar 2023

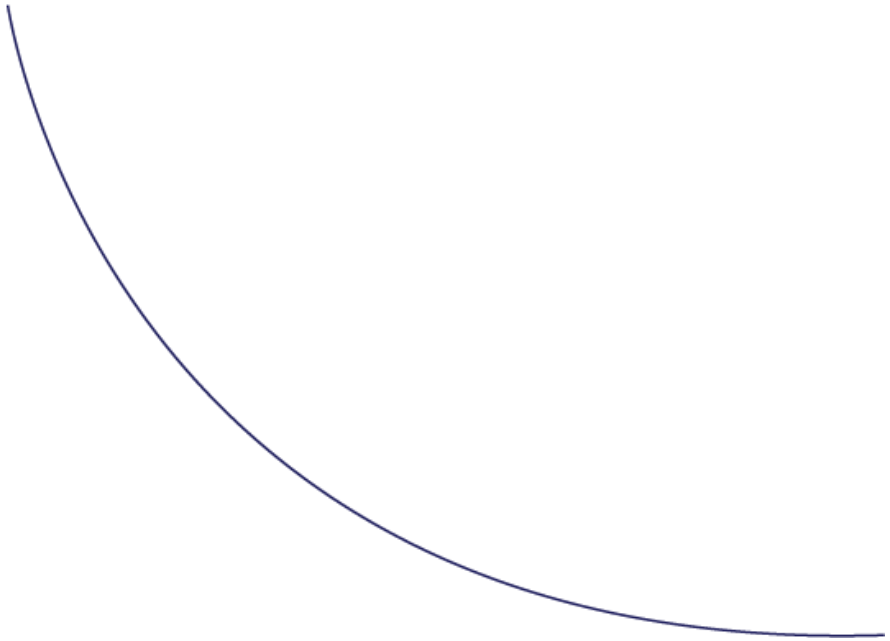
Isikuandmete töötlemise põhimõtted

- Seaduslikkus, õiglus ja läbipaistvus
- Eesmärgi piirang
- Võimalikult väheste andmete kogumine
- Õigsus
- Säilitamise piirang
- Usaldusväärsus ja konfidentsiaalsus

Seaduslik alus

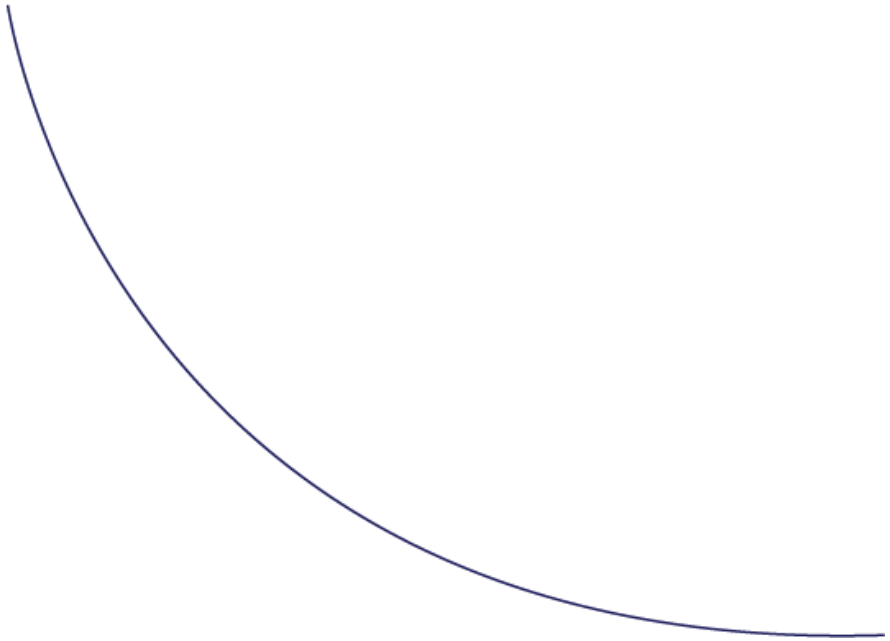
- andmesubjekt on andnud nõusoleku töödelda tema isikuandmeid ühel või mitmel konkreetsel eesmärgil
- isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele
- isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks
- isikuandmete töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks
- isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks
- isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps.

Nõusoleku andmise tingimused



- Kui töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik tõendada, et andmesubjekt on nõustunud oma isikuandmete töötlemisega.
- Nõusoleku andmine peab olema vabatahtlik.
- Kui andmesubjekt annab nõusoleku kirjaliku kinnitusena, mis puudutab ka muid küsimusi, esitatakse nõusoleku taotlus viisil, mis on muudest küsimustest selgelt eristatav, ning arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt. Sellise kinnituse mis tahes osa, mille puhul on tegemist GDPRi nõuete rikkumisega, ei ole siduv.
- Andmesubjektil on õigus oma nõusolek igal ajal tagasi võtta. Nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust.
- Nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine.

Õigustatud huvi



- Näiteks olukorras, kus andmesubjekt on vastutava töötleja klient või töötaja: õigustatud huvi edastada kliendi või töötaja isikuandmeid kontserni piires sisehalduse eesmärkidel.
- Õigustatud huvi olemasolu tuleb hoolikalt hinnata, sealhulgas seda, kas andmesubjekt võib andmete kogumise ajal ja kontekstis mõistlikkuse piires eeldada, et isikuandmeid võidakse sellel otstarbel töödelda.
- Vastutav töötleja peaks tõendama, et tema mõjuvad õigustatud huvid kaaluvad üles andmesubjekti huvid või põhiõigused ja –vabadused. Vaja läbi viia õigustatud huvi hindamine (ja see dokumenteerida).
- Läbipaistvus andmesubjekti ees: kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil f (õigustatud huvi), siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta.

Isikuandmete töötlemistoimingute registreerimine (RoPA)

Registreerimine on kirjalik, sealhulgas elektrooniline ja selles peab sisalduma:

- vastutava töötleja ning asjakohasel juhul kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed;
- töötlemise eesmärgid;
- andmesubjektide kategooriate ja isikuandmete liikide kirjeldus;
- vastuvõtjate kategooriad, kellele isikuandmeid on avalikustatud või avalikustatakse, sealhulgas kolmandates riikides olevad vastuvõtjad ja rahvusvahelised organisatsioonid;
- kui isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis andmed selle kohta koos asjaomase kolmanda riigi või rahvusvahelise organisatsiooni nimega, ning juhul, kui tegemist on GDPR artikli 49 lõike 1 teises lõigus osutatud edastamisega, siis sobivate kaitsemeetmete kohta koostatud dokumendid;
- võimaluse korral eri andmeliikide kustutamiseks ette nähtud tähtajad;
- võimaluse korral GDPR artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus.

Isikuandmete töötlemistoimingute registreerimine (RoPA)

RoPA kohustus kohaldub kõigile isikuandmete töötlejatele, välja arvatud vähem kui 250 töötajaga ettevõtjale või organisatsioonile, välja arvatud juhul, kui tema teostatav töötlemine kujutab endast tõenäoliselt ohtu andmesubjekti õigustele ja vabadustele, **töötlemine ei ole juhtumipõhine** või töödeldakse artikli 9 lõikes 1 osutatud isikuandmete eriliike või artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmeid.

Meelespea isikuandmete töötlejale

- Kohustused kõigil, kes töötlevad isikuandmeid
- Andmekaitse on pidev kohustus – siseeeskirju, dokumentatsiooni ja kaitsemeetmeid peab pidevalt kaasajastama; töödeldavad isikuandmed peavad olema õiged ja asjakohased
- Järgige isikuandmete töötlemise põhimõtteid ja olge andmesubjekti ees läbipaistvad

Kui on küsimusi, võta ühendust!

Kirsi Koistinen

kirsi.koistinen@sorainen.com

Lõimitud ja vaikimisi andmekaitse töötlemise turvalisuse tagamisel

SORAINEN

Kaupo Lepasepp
Tallinn

14. veebruar 2023

Lõimitud ja vaikimisi andmekaitse nõue
/ Data Protection By Design and By Default (DPbDD)

- Lõimitud ja vaikimisi andmekaitse:
  - Lõimitud: andmekaitse põhimõtted on töötlemise aluseks ja osaks üle kogu töötlemise ja infosüsteemi elutsükli
  - Vaikimisi: vaikimisi töödeldakse ainult vajalikke andmeid õiguspärase eesmärgi saavutamiseks vajalikus ulatuses
- Eesmärk tagada asjakohaste kaitsemeetmete rakendamine organisatsiooni infotehnoloogias ja töökorralduses.
- Kohustus kõigil vastutavatel töötlejatel olenemata organisatsiooni suurusest (sh SME-d).
- Dokumenteerimiskohustus põhimõtete rakendamise kohta.

Lõimitud ja vaikimisi andmekaitse

GDPR artikkel 25

1. Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning **töötlemise laadi, ulatust, konteksti ja eesmärke**, samuti töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte, rakendab vastutav töötleja **nii töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid**, nagu pseudonümiseerimine, mis on vajalikud andmekaitsepõhimõtete (nagu võimalikult väheste andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse, et täita käesoleva määruse nõudeid ja kaitsta andmesubjektide õigusi. / *lõimitud andmekaitse /*

2. Vastutav töötleja rakendab **asjakohaseid tehnilisi ja korralduslikke meetmeid**, millega tagatakse, et **vaikimisi töödeldakse ainult isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks**. See kehtib **kogutud isikuandmete hulga, nende töötlemise ulatuse, nende säilitamise aja ja nende kättesaadavuse suhtes**. Nende meetmetega tagatakse eelkõige see, et isikuandmeid ei tehta vaikimisi ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks. */vaikimisi andmekaitse/*

Riski- ja mõjupõhine lähenemine andmetöötluse turvalisuse tagamisel

- Lõimitud ja vaikimisi andmekaitse nõuete tagamine läbi riski- ja mõjupõhise lähenemise / riskianalüüsi.
- Riske hinnatakse **andmesubjekti vaatenurgast**, eesmärk on kaitsta andmesubjektide privaatsust.
- Süstemaatilisus ja põhjalikkus on olulised elemendid riskihinnangu läbiviimisel.
- Riske tuleb hinnata objektiivse hindamise põhjal, võttes arvesse riskide esinemise tõenäosust ja raskust.
- Arvesse tuleb võtta andmetöötluse laadi, ulatust, konteksti ja eesmärke (RISKID).
- Töötlemise ja meetmete kavandamine ja rakendamine riskianalüüsi alusel (MEETMED).
- Kulud on üks meetmete valiku kriteeriume. Suured kulud ei õigusta isiku privaatsuse kaitseta jätmist (kaaluda töötlemisest loobumist).
- Andmesubjekti teavitamine riskidest ja ohtudest („jääkrisk“).
- Riskianalüüsi, protsessi ja meetmete dokumenteerimine.
- Riskianalüüs on elutsüklit saatev protsess, mitte ühekordne tegevus.

Riskipõhine lähenemine

GDPR artikkel 32

1. Võttes arvesse **teaduse ja tehnoloogia viimast arengut** ja rakendamise kulusid ning arvestades isikuandmete töötlemise **laadi, ulatust, konteksti ja eesmärke**, samuti erineva tõenäosuse ja suurusega **ohte füüsiliste isikute õigustele ja vabadustele**, rakendavad vastutav töötleja ja volitatud töötleja **ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid**, hõlmates muu hulgas vastavalt vajadusele järgmist:

a) isikuandmete pseudonümiseerimine ja krüpteerimine;

b) võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;

c) võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral;

d) tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks.

2. Vajaliku turvalisuse taseme hindamisel **võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, eelkõige edastatavate, salvestatavate või muul viisil töödeldavate isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu**.

Asjakohased tehnilised ja korralduslikud meetmed

GDPR preambula 78

Füüsiliste isikute õiguste ja vabaduste kaitsmine isikuandmete töötlemisel eeldab **asjakohaste tehniliste ja korralduslike meetmete võtmist**, et tagada käesoleva määruse nõuete täitmine. Selleks et **olla võimeline tõendama käesoleva määruse täitmist**, peaks vastutav töötleja **võtma vastu sise-eeskirjad ja rakendama meetmeid,** mis vastavad eelkõige lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtetele.

Sellised meetmed võivad koosneda muu hulgas isikuandmete töötlemise miinimumini viimisest, isikuandmete võimalikult kiirest pseudonümiseerimisest, läbipaistvusest seoses isikuandmete eesmärgi ja töötlemisega, andmesubjektile andmete töötlemise jälgimise võimaluse andmisest, vastutavale töötlejale võimaluse andmisest **luua ja parandada turvameetmeid**.

Selliste rakenduste, teenuste ja toodete väljatöötamisel, kavandamisel, valimisel ja kasutamisel, mis põhinevad isikuandmete töötlemisel või mille käigus töödeldakse isikuandmeid nende ülesannete täitmiseks, tuleks nende toodete, teenuste ja rakenduste tootjaid innustada võtma selliste toodete, teenuste ja rakenduste väljatöötamisel ja kavandamisel arvesse õigust andmekaitsele ning tagama asjakohaselt teaduse ja tehnoloogia viimast arengut arvestades, et vastutavad töötlejad ja volitatud töötlejad saaksid täita oma andmekaitsealaseid kohustusi. [...]

Lõimitud ja vaikimisi andmekaitse elemendid

- Läbipaistvus */ Transparency*
- Õiguspärasus */ Lawfulness*
- Õiglus */ Fairness*
- Eesmärgi piirang */ Purpose Limitation*
- Võimalikult väheste andmete töötlemine / *Data Minimisation*
- Õigsus */ Accuracy*
- Säilitamise piirang */ Storage Limitation*
- Usaldusväärsus ja konfidentsiaalsus */ Integrity & Confidentiality*
- Vastutus */ Accountability*

Privaatsust edendavad tehnoloogiad

/Privacy-enhancing technologies (PETs)

- Vahendid innovatsiooni ja eraelu puutumatuse tasakaalustamiseks.
- Süsteemne ja põhjalik toetus andmekaitsepõhimõtete rakendamisel.
- Olemasolevaid tehnoloogiad on väga erinevad, ja tuleb teha teadlik valik sobiva tehnoloogia kasutuselevõtuks.
- Olemas üldistatud tasemega juhised, aga tehnoloogia (sh PET) valik on (vastutava) töötleja vastutus

Andmetöötluse meelespea

- Põhjalik riskihinnang võimaldab teha kindlaks andmetöötluse riskid ja neid efektiivselt maandada.
- Andmetöötluse raames tuleb järgida (ja dokumenteerida) lõimitud ja vaikimisi andmekaitse põhimõtteid.
- Privaatsust suurendavad tehnoloogiad aitavad minimiseerida andmesubjekte varitsevaid riske.
- Vastutatav töötleja peab tundma enda ja volitatud töötlejate tehnoloogiliste süsteemide omadusi

Kui on küsimusi, võta ühendust!

Kaupo Lepasepp

kaupo.lepasepp@sorainen.com

Mida silmas pidada teenusepakkujate ja koostööpartnerite kaasamisel

SORAINEN

Mihkel Miidla
Tallinn

14.02.2023

Millest alustada?

- Analüüsi olukorda
  - Koostöö/teenuse sisu
  - Mis andmed liiguvad, miks ja kuhu?
  - Õiguslik alus?
  - Milline on olemasolev dokumentatsioon
- Kas uus teenusepakkuja?
- Juba olemasolev?

Koostööpartneri /teenusepakkuja roll (konkreetse töötlemise eesmärgi raames)

- Vastutav töötleja?
- Kaasvastutav töötleja?
- Volitatud töötleja?

- + Milline on meie endi roll?

Auditeerimiskohustus ja vastutuse põhimõte

- GDPR Art 28 (1): *„[...] kasutab vastutav töötleja ainult selliseid volitatud töötlejaid, **kes annavad piisava tagatise**, et nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid [...] “*
- *Vastutav töötleja vastutab GDPRi nõuete täitmise eest ja peab olema võimeline nõuete täitmist tõendama*

Lepingud

- Andmete töötlemise leping volitatud töötlejaga (DPA)
- Leping teise vastutava töötlejaga andmete edastamiseks
- Leping kaasvastutavate töötlejate vahel
- Kohustuslikud teemad, mida peab lepingus käsitlema.

Andmete edastamine väljapoole EMP-d?

- Isikuandmete edastamine väljapoole EL/EMP-d või riiki, milles pole tagatud piisav andmekaitse tase
- Andmete eksportija ja -importija
- *Schrems II*
- EK mudelleping (SCC)
  - Andmeedastuse mõjuhinnang (DTA)
    - Andmete importija peab suutma SCC-d täita (kohalik õigus ja tavad ei tohi seda takistada)
    - Vajadusel täiendavad kaitsemeetmed
    - Vt ka Euroopa Andmekaitsenõukogu soovitusi
- Eriliigiliste andmete edastamise korral, vaata enne ka asjakohase liikmesriigi õigust – sellest võivad tuleneda täiendavad keelud, piirangud ja kohustused.
- Sektoripõhised reeglid/piirangud

Pilv

- Põhitegevust võimaldav või toetav pilvepõhine teenus?
- Oluline on aru saada teenuse sisust, andmete liikumisest ja sellest, mida ütlevad (tüüp)tingimused ja –lepingud.
- Kuidas puudused kõrvaldada?

Edasi?

- Protsessid koostööpartnerite / teenusepakkujate kaasamiseks
- Protsessid koostööpartneritega / teenusepakkujatega suhte lõppemisel

- Standarddokumentatsioon
- Uuenda RoPA
- Vajadusel LIA / DPIA
- Taga läbipaistvus (privacy policy uuendamine)

- Pidev protsess

Kui on küsimusi, võta ühendust!

Mihkel Miidla

mihkel.miidla@sorainen.com

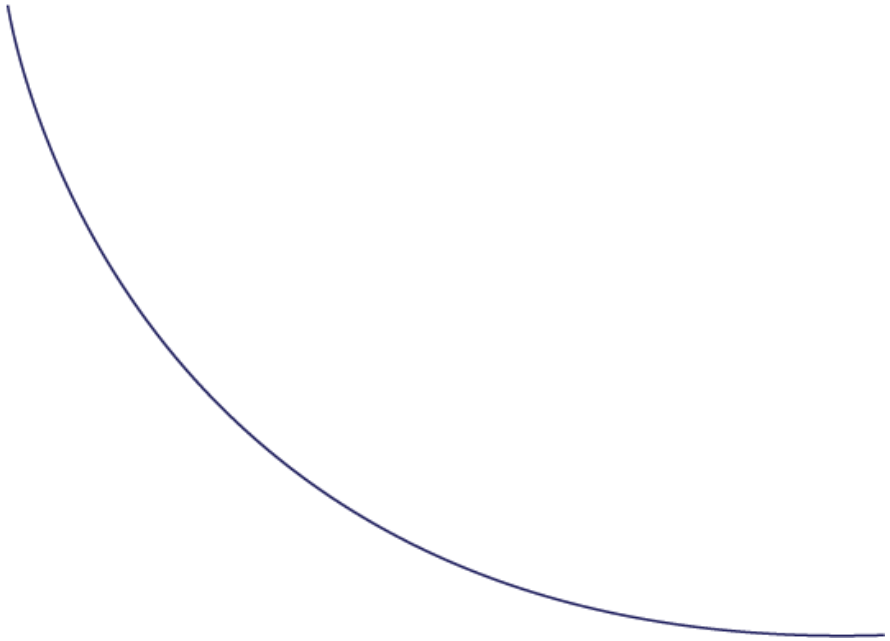
Ümmargune GDPR: „oht“, „suur oht“, „ulatuslik“, „korrapärane“ ja „süstemaatiline“ töötlemine

SORAINEN

Liisa Maria Kuuskmaa
Advokaat

14.02.2023

Määratlemata õigusmõisted



- Andmeleketest teavitamise kohustused
  - **Oht** ja **suur oht** andmesubjektidele
- Andmekaitsealase mõjuhinnangu tegemise kohustus
  - **Suur oht** andmesubjektidele
  - **Süstemaatiline** ja **ulatuslik** isiklike aspektide automatiseeritud hindamine
  - **Ulatuslik** delikaatsete isikuandmete töötlemine
- Andmekaitseametniku määramise kohustus
  - **Ulatuslik** andmesubjektide **korrapärane** ja **süstemaatiline** jälgimine põhitegevusena
  - **Ulatuslik** delikaatsete isikuandmete töötlemine

Isikuandmetega seotud rikkumisest teavitamine

Artikkel 33

1. Isikuandmetega seotud rikkumise korral teatab vastutav töötleja isikuandmetega seotud rikkumisest artikli 55 kohasele pädevale järelevalveasutusele põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist, **välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele**. Kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus.

/.../

Artikkel 34

1. Kui isikuandmetega seotud rikkumine **kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele**, teavitab vastutav töötleja andmesubjekti põhjendamatu viivituseta isikuandmetega seotud rikkumisest.

/.../

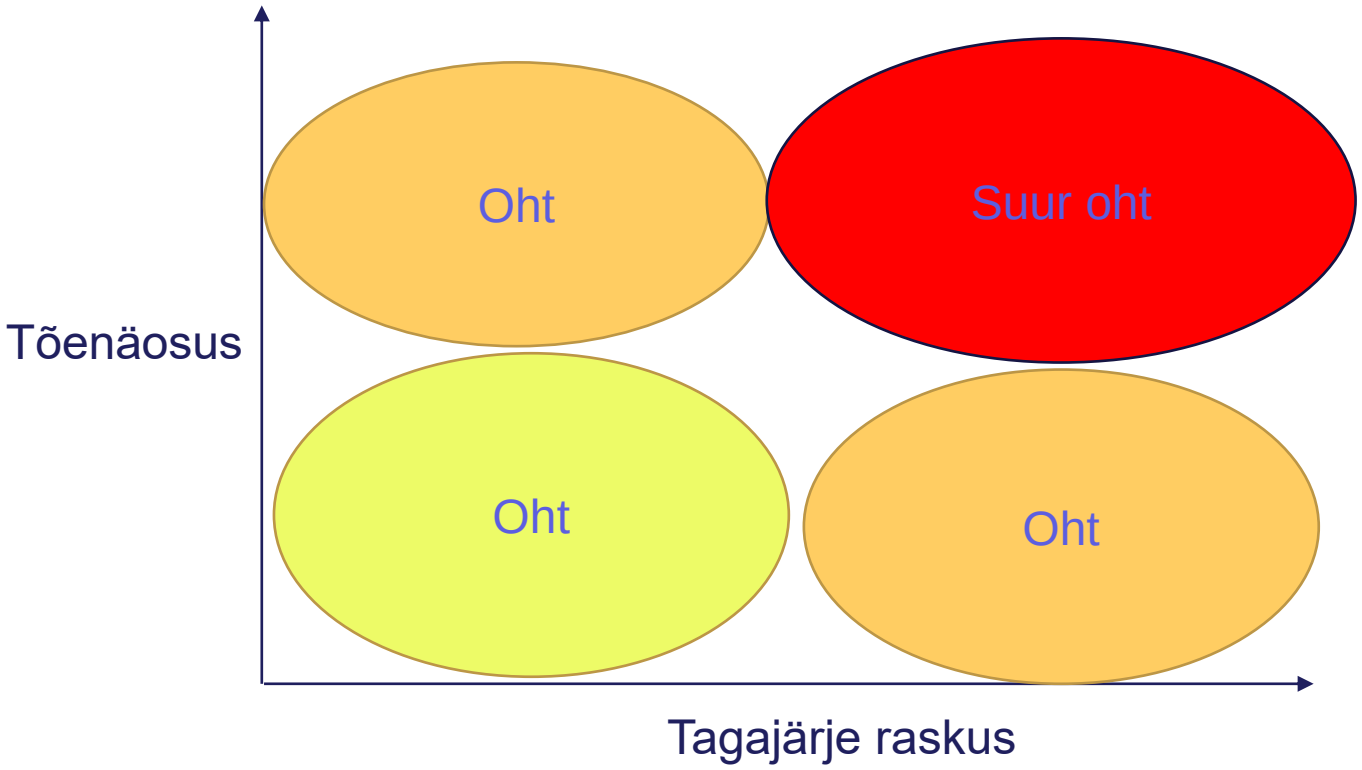
3. Lõikes 1 osutatud andmesubjekti teavitamist ei nõuta juhul, kui on täidetud järgmised tingimused.

a) vastutav töötleja on kehtestanud asjakohased tehnilised ja korralduslikud kaitsemeetmed ja neid kohaldati isikuandmetega seotud rikkumisest mõjutatud isikuandmetele, kasutades eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsuõiguseta isikutele loetamatuks (näiteks krüpteerimine);

b) vastutav töötleja on võtnud hilisemad meetmed, mis tagavad, et lõikes 1 osutatud **suure ohu teke andmesubjektide õigustele ja vabadustele ei ole enam tõenäoline**, või

c) see nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse muu sarnane meede, millega teavitatakse kõiki andmesubjekte võrdselt tulemuslikul viisil.

Riskide hindamine



Riskide hindamine andmesubjekti vaatenurgast!

Füüsiline, varaline või mittevaraline kahju

Andmekaitsealase mõjuhinnangu tegemise kohustus

Artikkel 35

1. Kui teatavat tüüpi isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete **töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht**, hindab vastutav töötleja enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsele. Endast sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata koos.

/.../

3. Lõikes 1 osutatud andmekaitsealase mõjuhinnangu tegemine on nõutav juhtudel:

a) **füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine**, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut;

b) artikli 9 lõikes 1 osutatud andmete **eriliikide** või artiklis 10 osutatud **süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmete ulatuslik töötlemine**, või

c) **avalike alade ulatuslik süstemaatiline jälgimine**.

4. Järelevalveasutus koostab ja avalikustab selliste isikuandmete töötlemise toimingute tüüpide loetelu, mille suhtes kohaldatakse lõike 1 kohast nõuet teha andmekaitsealane mõjuhinnang. Järelevalveasutus edastab need loetelud artiklis 68 osutatud andmekaitsenõukogule.

5. Järelevalveasutus võib samuti koostada ja avaldada selliste isikuandmete töötlemise toimingute tüüpide loetelu, mille puhul ei ole andmekaitsealane mõjuhinnang nõutav. Järelevalveasutus edastab need loetelud andmekaitsenõukogule.

/.../

Artikkel 36

1. Vastutav töötleja **konsulteerib enne isikuandmete töötlemist järelevalveasutusega**, kui artikli 35 kohasest **andmekaitsealasest mõjuhinnangust nähtub**, et isikuandmete töötlemise tulemusena **tekiks vastutava töötleja poolt ohu leevendamiseks võetavate meetmete puudumise korral suur oht**.

Andmekaitseametniku määramise kohustus

Artikkel 37

1. Vastutav töötleja ja volitatud töötleja määravad andmekaitseametniku, kui

a) isikuandmeid töötleb avaliku sektori asutus või organ, välja arvatud oma õigust mõistvat funktsiooni täitvad kohtud;

b) vastutava töötleja või volitatud töötleja **põhitegevuse** moodustavad isikuandmete töötlemise toimingud, mille **laad, ulatus ja/või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise**, või

c) vastutava töötleja või volitatud töötleja **põhitegevuse** moodustab artiklis 9 osutatud andmete **eriliikide** ja artiklis 10 osutatud süüteoasjades **süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine**.

Süstemaatiline

Täidetud vähemalt üks järgmistest tingimustest:

- toimub vastavalt süsteemile,
- ettevalmistatud, korraldatud või metoodiline,
- üldise andmete kogumise kava osa,
- strateegia osa.

Regulaarne

Täidetud vähemalt üks järgmistest kriteeriumitest:

- Toimub pidevalt või kindlate ajavahemike ajalt kindla perioodi jooksul
- Toimub kindlaksmääratud aegadel
- Toimub pidevalt või perioodiliselt

Ulatuslik

AKI siseriiklikud kriteeriumid

Igakordselt arvesse võtta järgmist:

- Andmesubjektide arv või osakaal asjaomases populatsioonis
- Andmete maht ja/või ulatus
- Töötlemise kestus või pidevus
- Töötlemise geograafiline ulatus

https://www.aki.ee/et/eraelu-kaitse/mojuhinnangu-tegemine

Oht hõlmab sündmust ja selle tagajärgi ning seda hinnatakse mõju, tõenäosuse ja inimese vaatenurgast. Töötlemise ulatuslikkuse ja süsteemsuse määratlemisel tuleb aga andmetöötlejal lähtuda kindlatest kriteeriumidest.

Siseriikliku andmetöötluse juures määrab ulatuslikkuse kriteeriumi kohalik andmekaitseasutus. Eestis on selleks Andmekaitse Inspektsioon.

Kui Eesti vastutava andmetöötleja tegevus ulatub lisaks veel näiteks Lätti, tuleb aga järgida Euroopa andmekaitsenõukogu kinnitatud vastavaid kriteeriume. Kõikide Euroopa liikmesriikide piiriülest andmetöötlust puudutavate mõjuhinnangute nimekirjad on koostatud sarnasel põhimõttel ja kooskõlastatud Euroopa Andmekaitsenõukoguga.

Eestis on siseriikliku mõjuhinnangu ulatuslikkuse kriteeriumid järgnevad:

- eriliiki või süüteoandmeid 5000 ja enama inimese kohta;
- suurt ohtu põhjustavaid andmeid 10 000 ja enama inimese kohta;
- ülejäänud isikuandmed 50 000 ja enama inimese kohta.

Mõjuhinnangu tegemise kohustust ei ole andmetöötlusele, mis on olnud kasutusel juba enne isikuandmete kaitse üldmääruse kehtima hakkamist.

https://ec.europa.eu/newsroom/article29/items/612048/en

Suunised andmekaitseametnike kohta

Vastu võetud 13. detsembril 2016

Viimati muudetud ja vastu võetud 5. aprillil 2017

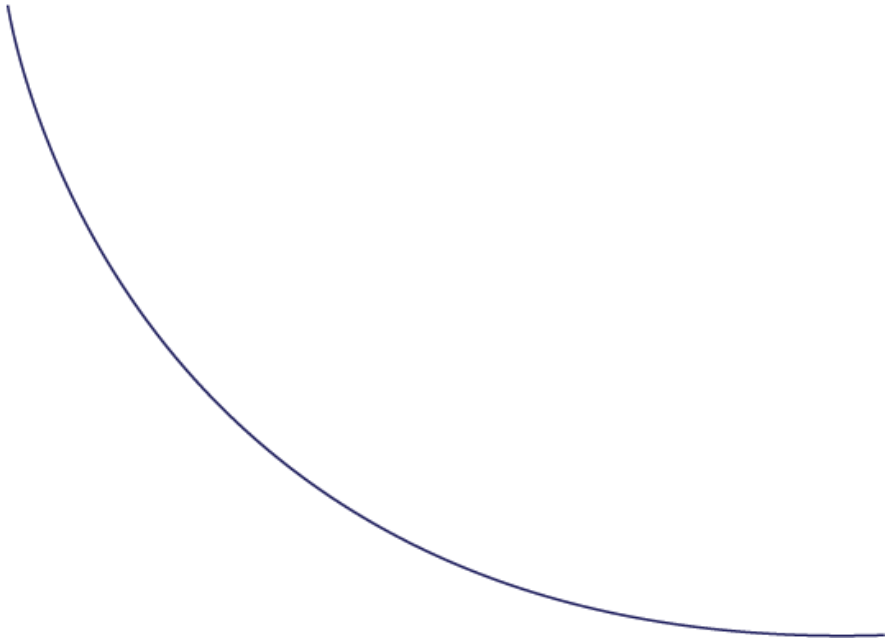
https://ec.europa.eu/newsroom/article29/items/611236

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

Tõenäoliselt suur oht (üldjuhul vähemalt 2 kriteeriumit, erandjuhul ka 1)



- Hindamine, sh profiilianalüüsi tegemine ja prognoosotsused
- Õiguslike või samaväärsete tagajärgedega automatiseeritud otsused
- Süstemaatiline jälgimine
- Tundlikud või väga isiklikud andmed
- Ulatuslik töötlemine
- Andmekogude sobitamine või kombineerimine
- Haavatavad andmesubjektid (nt lapsed, töötajad, varjupaigataotlejad, eakad, patsiendid, vaimselt haiged inimesed jt)
- Uuenduslikud lahendused, uued tehnoloogiad
- Töötlemine takistab andmesubjektidel õiguse või teenuse või lepingu kasutamist (nt krediidiotsused)

Kui on küsimusi,
võta ühendust:

Liisa Maria Kuuskmaa
liisa.kuuskmaa@sorainen.com

Kuidas turundada järelevalveasutustele hambusse jäämata? Kolme Balti riigi vaade

SORAINEN

Otseturustus – mis see on?

- SMS
- Telefonikõned
- Robotkõned
- LinkedIn/WhatsApp sõnumid
- Uudiskirjad
- E-kirjad
- Tavapost

Nõuded elektrooniliste kontaktandmete otseturustuseks kasutamisele

- E-privaatsuse direktiiv + kohalikud iseärasused
  - Eestis elektroonilise side seaduse § 103^1
- Elektroonilised kontaktandmed on andmed, mis võimaldavad elektroonilise side võrgu kaudu edastada isikule teavet, sealhulgas faksi, elektronposti või lühi- ja multimeediasõnumiga

ESTONIA

Opt-in for individuals, *unless you have already sold a product or provided a service to the individual and thereby received his/her contacts, and you wish to use these contacts for direct marketing of similar products or services to the same person.*

Opt-out for B2B

Multi-party voice calls in real time,

unless the natural person has expressly forbidden this.

General rules for advertising and fair commercial practice must be met

Name of the sender

Simple withdrawal

LATVIA

Opt-in for individuals, *unless you have already sold a product or provided a service to the individual and thereby received his/her contacts, and you wish to use these contacts for direct marketing of similar products or services to the same person.*

Opt-out for B2B

No public black list

Cold calls – ok (withdrawal must be respected)

General rules for advertising and fair commercial practice rules must be met

Name of the sender

Simple withdrawal

LITHUANIA

Opt-in for individuals, *unless you have already sold a product or provided a service to the individual and thereby received his/her contacts, and you wish to use these contacts for direct marketing of similar products or services to the same person*

Opt-in for B2B

No cold calls

Calls for both B2C and B2B only with prior consent

General rules for advertising and fair commercial practice rules must be met

Name of the sender

Simple withdrawal

Questions

- How to deal with the contact data of the board members of a legal entity in the context of direct marketing?
- Can we share contact data within the group for direct marketing?
- What if two entities merge – can the new legal body use/rely on the database collected by merging entities?

Lise-Lotte Lääne

Estonia

lise-lotte.laane@sorainen.com

Irma Kirklytė

Lithuania

irma.kirklyte@sorainen.com

Jūlija Terjuhana

Latvia

julija.terjuhana@sorainen.com

Küsi meilt nõu!

kirsi.koistinen@sorainen.com

kaupo.lepasepp@sorainen.com

mihkel.miidla@sorainen.com

liisa.kuuskmaa@sorainen.com

lise-lotte.laane@sorainen.com

irma.kirklyte@sorainen.com

julija.terjuhana@sorainen.com