Kes peavad mõjuhinnangu tegema? Mõjuhinnangu peavad tegema kõik andmetöötlejad, kelle isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsilistele isikute õigustele ja vabadustele suur oht. **Kohustus** mõjuhinnangu tegemiseks on, kui toimub:

- isiklike aspektide (nt isiku vaated, seisukohad, isikuomadused, harjumused, huvid, eelistused, sotsiaalne staatus, käitumine, asukoht, liikumine) 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;
- isikuandmete eriliikide (nt terviseandmed) ulatuslik töötlemine, või
- avalike alade ulatuslik süstemaatiline jälgimine (nt kaamerate kasutamine valve-või korrakaitse eesmärgil).

AKI hinnangul on suure ohuga tegemist nt kui töödeldakse terviseandmeid haiglates ja tervisekeskustes või toimub isikuandmete edastamine välisriikidesse. Vt täpsemalt siit.

Mõjuhinnang peab hõlmama vähemalt järgmist:

a) süsteemne (kogu süsteemi hõlmav) kirjeldus kavandatud isikuandmete töötlemise toimingutest ja töötlemise eesmärkidest.

b) hinnang, kas isikuandmete töötlemine on vajalik ja proportsionaalne eesmärkide suhtes.

c) riskide hindamine, mis võivad ohustada füüsiliste isikute õigusi ja vabadusi.

d) kavandatud meetmed riskide käsitlemiseks, sealhulgas nõuded, protseduurid ja süsteemid, mis tagavad isikuandmete kaitse ning kinnitavad vastavust isikuandmete kaitse määrusele, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.

Kui andmekaitsealane mõjuhinnang näitab, et isikuandmete töötlemise toimingutega kaasneb suur oht, mida ei saa leevendada kättesaadava tehnoloogia ja rakendamise maksumuse osas asjakohaste meetmetega, tuleks enne töötlemist konsulteerida AKI-ga.

Allikas: EL määrus 2016/679 artikkel 35 lõiked 1 ja 7, preambula p 84 ja p 94, artikkel 36 lõige 1

Andmekaitsealane mõjuhinnang – näidisdokument

Kokkuvõte andmekaitsealase mõjuhinnangu tulemustest

Lühike kommentaar andmekaitsealase mõjuhinnangu tulemustest.

- *Andmesubjektide tutvustus*
- *Mõjuhinnangu ajaline kestus/ skoop*
- *Muud olulised asjaolud, mida tahetakse välja tuua*
- *Järeldused*

Järgneb nimekiri riskidest/leidudest, mis tuvastati andmekaitse mõjuhinnangu läbiviimise tulemusena.

Riski number	***Riski nimetus***	***Riski tase***	***Ettepanek riski maandamiseks***
1	*[Riski kokkuvõttev nimetus]*	*[Madal, Keskmine, Kõrge]*	*[Kasutusele võtta..]*
2	*[Riski kokkuvõttev nimetus]*	*[Madal, Keskmine, Kõrge]*	*[Aktsepteerida riski, täiendavaid meetmeid ei võeta kasutusele.]*
…			

1. Sissejuhatus

Siin kirjeldage lühidalt asutuse tegevust.

Kirjeldage lühidalt andmesubjekte, kelle andmeid töödeldakse (üldine sissejuhatus andmesubjektidest).

1.1. Mis on andmekaitsealane mõjuhinnang?

Andmekaitsealane mõjuhinnang on tööriist, mis kirjeldab, kuidas süsteemis/protsessis töödeldakse isikuandmeid ning tagatakse isikuandmete kaitse. Mõjuhinnang aitab hinnata töötlemisega seotud riske. Käesoleva tööriista kasutamine võimaldab süsteemis/protsessis tuvastada andmekaitsealaseid puudusi ning anda soovitusi puuduste kõrvaldamiseks.

Oluline on tähele panna, et:

- käesolev mõjuhinnang viiakse süsteemi/protsessi kohta läbi üksnes andmekaitse kontekstis, võttes arvesse kehtivaid andmekaitse põhimõtted, parimaid praktikaid, avaldatud tegevusjuhiseid, õigusakte ning asjassepuutuvaid direktiive ja määruseid;
- asjaomased isikud või otsustajad peavad olema andmekaitsealase mõjuhinnangu tulemusena informeeritud, kuidas süsteemis/protsessis töödeldakse isikuandmeid ning kas isikuandmete kaitse on tagatud nõutaval määral. Andmekaitsealase mõjuhinnangu läbiviimine peab olema ajastatud selliselt, et eelseisvas otsustusprotsessis saaks arvesse võtta hindamise tulemusi või leide;
- andmekaitsealane mõjuhinnang ei saa olla ühe inimese looming, vaid koostöös loodav dokument;
- andmekaitsealane mõjuhinnang on elav dokument – seda uuendatakse iga kord, kui isikuandmete töötlemises tehakse muudatusi (näiteks uuendatakse tarkvara, võetakse kasutusele uus tehnoloogia, muutub ökosüsteem ja ilmnevad uued riskid vms).
- andmekaitsealane mõjuhinnang on protsess, mis on osa tehnilisest ja organisatsioonilisest kultuurist.

Andmekaitsealane mõjuhinnang peab olema:

- koostatud spetsiaalselt Teie organisatsioonile ja arvestades teie organisatsiooni spetsiifikat (võttes arvesse isikuandmete töötlemise laadi, konteksti, ulatust ja eesmärke) – puudub kõigile sobiv mõjuhinnangu dokumendi vorm.
- selge ja arusaadav – kasutage korrektseid väljendeid ja vältige mitmetähenduslikkust. Andmekaitsealast mõjuhinnangu dokumenti ei koostata üksnes AKI-le, vaid sellest peavad aru saama kõik organisatsiooni asjassepuutuvad isikud.
- põhjalik – tähelepanu tuleb pöörata kõikidele riskidele. Konsulteerige paljude organisatsiooni spetsialistidega (näiteks projektijuhiga, andmekaitse spetsialistiga, IT arendajaga, kasutajatoe töötajaga vms). Dokumendi sisend ei ole ainult tehniline, vaid tähelepanu tuleb pöörata sellele, milline on organisatsioonis tegelik praktika.

1.2. Mõjuhinnangu läbiviimisest

1.2.1. Läbiviimise aeg

Käesolev andmekaitsealane mõjuhinnang on läbi viidud ajavahemikul *00.00.0000 – 00.00.0000*.

1.2.2. Mõjuhinnangu ulatus

Kirjeldada läbiviimise ulatust või skoopi.

[Kas andmekaitsealane mõjuhinnang hõlmab tervet organisatsiooni tegevust või on see koostatud ühe toote/protsessi elutsükli kohta?]

1.2.3. Metoodika

Kirjelda kasutatud metoodikat.

- Metoodika valik on vaba – kohustuslikku metoodikat ei ole.
- Metoodika valikul tuleb arvesse võtta andmetöötlemise iseloomu, ulatust ja konteksti.
- Andmekaitsealane mõjuhinnang eeldab üldiselt riskil põhineva meetodi kasutamist – riskid tuleb identifitseerida ja hinnata. Riskianalüüsis on soovitatav kasutada hindamiseks riski realiseerumise tõenäosust ja mõju (võimalikud tagajärjed). Võib kasutada mõnda ISO-standardi sarnast riskihindamise metoodikat.

2. Infosüsteemi kirjeldus

Lühike sissejuhatus alateemasse.

Võimalusel kasutada olemasolevat arhitektuuridokumenti või sellele viidata.

2.1. *Süsteemi kasutusotstarve*
2.2. *Tugisüsteemid (support tiers)*
2.3. *Informatsiooni elutsükkel (lifecycle)*
2.4. *Kasutajad ja nende rollid*
2.5. *Infosüsteemi arhitektuur*

Infosüsteemi kohta käivad alapealkirjad/teemad on siin indikatiivsed – alateemad olenevad organisatsiooni infosüsteemi spetsiifikast ning kokku tuleb panna teie organisatsiooni jaoks sobiv teemadegrupp. Eesmärk on võimalikult arusaadavalt selgitada süsteemi olemust ja isikuandmetesse puutuvat selles. Alateemadena võib kasutada näiteks:

- Kasutajaks registreerimine
- Isikuandmete allikad
- Andmejoad
- Teadaolevad turvameetmed
- Olemasolev riskidokumentatsioon
- Toetavad mudelid
- jne

3. Isikuandmete töötlemise toimingud

Mis on tänane olukord? Mis muutub?

3.1. Isikuandmete kogumine

- *Kirjeldage andmesubjekte (sh alaealised)*
- *Andmekoosseisud*
- *Kuidas andmekogumise protsess töötab?*
- *Andmete muutmine, lisamine.*
- *Andmete ühildamine ja ühendamine.*
- *Kuidas tagatakse andmete ajakohasus?*
- *Andmesubjekti nõusolek. Kuidas tõendatakse, et on andnud nõusoleku?*
- *Nõusoleku tagasivõtmine.*
- *Jms*

3.2. Isikuandmete säilitamine

- *Kuidas ja kus andmeid säilitatakse?*
- *Säilitamise tähtajad.*
- *Kuidas tagatakse, et andmeid säilitatakse seni, kuni see on vajalik töötlemise eesmärgi täitmiseks (avalikes huvides võib säilitada kauem, kui see vajalik näiteks teadusuuringute läbiviimiseks)?*
- *Hoiustamisel kasutatavad turvameetmed (ISKE)?*
- *Kuidas välditakse andmete juhuslikku hävimist või kahjustumist?*
- *Logid, turvakoopiad.*
- *Arhiveerimine.*
- *Arhiiviväärtusega andmed.*
- *jne*

3.3. Isikuandmete kasutamine

- *Millal, kelle poolt ja kuidas andmeid kasutatakse?*
- *Päringute tegemine.*
- *Andmete lugemine.*
- *Kättesaadavaks tegemine. Avalikustamine.*
- *Kättesaadavuse piiramine.*
- *Kuidas andmesubjektil on võimalik saada väljavõte andmetest, mida tema kohta on kogutud? Mis kujul see väljavõte antakse?*
- *Juurdepääs andmetele.*
- *Kuidas välditakse loata või ebaseadusliku juurdepääsu eest?*
- *jne*

3.4. Isikuandmete edastamine

- *Kas ja kellele andmeid edastatakse?*
- *Kuidas andmeid edastatakse?*

- *Kas andmesubjekt saab taotleda oma andmete ülekandmist teisele töötlejale (kui andmesubjekt esitas isikuandmed omaenda nõusoleku alusel või kui töötlemine on vajalik lepingu täitmiseks- seda ei kohaldata, kui töötlemine avalike kohustuste täitmiseks)?*
- *Kolmandatesse riikidesse edastamine?*
- *jne*

3.5. Isikuandmete kustutamine

- *Millal, kuidas ja kelle poolt andmeid kustutatakse?*
- *Hävitamine, blokeerimine.*
- *Kas andmesubjekt ise saab kasutada õigust taotleda oma andmete kustutamist (õigus „olla unustatud“)?*
- *Ebaõigete andmete muutmine või kustutamine?*
- *Kustutamise dokumenteerimine (logi selle kohta).*
- *jne*

4. Isikuandmete töötlemise eesmärgid

4.1. Töötlemise eesmärgid

- *Kirjeldage eesmärke, miks isikuandmeid kogutakse ja töödeldakse (näiteks avalikes huvides oleva ülesande täitmiseks – siis lisada õigusakti nimetus).*
- *Kas ja kuidas eesmärkidele vastavus tuvastatakse organisatsiooni poolt enne andmete kogumist või andmete kogumise ajal?*
- *Kuidas tagatakse, et andmeid töödeldakse üksnes neil eesmärkidel, milleks neid kogutakse?*
- *Kas andmeid töödeldakse ka muul viisil, mis on esialgsete töötlemise eesmärkidega vastuolus? Kelle poolt ja miks?*
- *jne*

4.2. Töötlemise vajalikkus ja proportsionaalsus

Mis põhjustel töödeldakse andmeid töötlemise eesmärkide saavutamiseks just sel viisil nagu seda praegu tehakse? Kas eesmärkide saavutamiseks on võimalik andmeid töödelda ka mõnel muul viisil? Kas on olemas lihtsam viis (tavaliselt see tähendab ka vähem riski põhjustav) eesmärkide saavutamiseks? Oluline on siin täpselt ja argumenteeritult selgitada, miks andmeid töödeldakse just sel viisil ja sellises ulatuses!

- *Minimaalsuse põhimõte (andmeid kogutakse üksnes ulatuses, mis on vajalik andmetöötluse eesmärkide täitmiseks)*
- *Täpsus, täielikkus ja ajakohasus*

- *Kas organisatsioon on avalikustanud on andmetöötluspõhimõtted, et andmesubjektid teaksid, organisatsiooni isikuandmete töötlemise põhimõtteid ja praktikat?*
- *Kas andmesubjektil endal on juurdepääs tema kohta kogutavale andmestikule?*
- *Jne*

5. Riskid ja nende maandamine

Kirjeldada riskid. Metoodikate juhendid on käesoleva dokumendi lisas.

Riski number	***Riski nimetus***	***Riski tõenäosus***	***Riski mõju***	***Riski tase***	***Lisamärkused***	***Ettepanek riski maandamiseks***
1	*[Riski kokkuvõttev nimetus]*	*[0-4]*	*[0-4]*	*[Kõrge, Keskmine, Madal]*	*[Kirjelda tähtsust omavad asjaolud]*	*[Maandada, kasutusele võtta..]*
2	*[Riski kokkuvõttev nimetus]*	*[0-4]*	*[0-4]*	*[Kõrge, Keskmine, Madal*	*[Kirjelda tähtsust omavad asjaolud]*	*[Aktsepteerida, täiendavaid meetmeid ei võeta kasutusele.]*
…						

<u>Ettepanek riski maandamiseks</u>

Strateegia kirjeldus riskiga edasi tegelemiseks (vältida, maandada, üle kanda, aktsepteerida).

Üldistatult on riskid need, mis võivad ohustada füüsilise isiku õigusi ja vabadusi. Risk on oletuslik stsenaarium, mis võib juhtuda. Täpsemalt öeldes – risk on asjaolu, mis võib põhjustada füüsilisele isikule füüsilist, materiaalset või mittevaralist kahju.

Andmekaitse kontekstis täpsemalt tähendab risk, et andmete töötlemise toimingute tulemusena on oht, et see võib põhjustada füüsilise isiku:

- diskrimineerimist;
- identiteedivargust või –pettust;
- rahalist kahju;
- maine kahjustamist;
- ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu;
- isikuandmete pseudonümiseerimise loata tühistamist (pseudonüümitud andmete lubamatu tagasipööramine);
- mõnda muud tõsist majanduslikku või sotsiaalset kahju;
- sõna- või teabevabaduse rikkumist;
- ettevõtlusvabaduse rikkumist;
- mõtte-, südametunnistuse- või usuvabaduse rikkumist.

Lisaks on füüsilisel isikul õigus:

- tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele;
- kontrollida oma isikuandmete kasutamist;

- hoida saladuses oma: etniline päritolu, rassiline kuuluvus, poliitilised vaated, usulised ja maailmavaatelised veendumused, ametiühingusse kuulumine, terviseseisundi või puude andmed, geneetilised andmed, seksuaalelu puudutavad andmed, andmed süüteo toimepanemise või selle ohvriks langemise kohta, turvalisust puudutavad andmed;
- kultuurilisele, usulisele ja keelelisele mitmekesisusele.

Riskideks peetakse veel:

- isikute andmete töötlemist, kes kuuluvad ühiskonna n.ö haavatavasse gruppi, näiteks lapsed, puuetega inimesed;
- töödeldakse korraga väga suurt hulka isikuandmeid ja riski realiseerumisel puudutaks see väga suurt hulka andmesubjekte;
- andmete automatiseeritud töötlemine, mis võib põhjustada isikule õiguslikke tagajärgi või on sellel muu ulatuslik mõju, nagu näiteks isikuandmete automatiseeritud töötlemisel põhinev profiilianalüüs, mille käigus hinnatakse füüsilise isikuga seotud isiklikke aspekte, mis on seotud töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega.

Ülaltoodud riskidel on lai tähendus – riskianalüüsis vajavad need sageli tõlkimist tehnoloogia keelde. Näiteks „sõnavabadus“ võib olla seotud selliste tehnoloogiliste mõistetega nagu „krüpteerimine“, „juurdepääsu kontrollimine“ või „autoriseerimine“. Seega tuleks dokumendi selles osas olla valmis põhjalikuks turvalisuse ja isikuandmete privaatsusnõuete analüüsiks.

Riskide maandamise juures on oluline märkida, et riski võib täielikult vältida (maandada) või vähendada aktsepteeritud tasemeni. Riskijuhtimise põhimõte on, et kõiki riske ei ole võimalik maandada nullini. Mõnikord lihtsalt aktsepteeritakse riski olemasolu - riski realiseerumise tõenäosus ja võimalik kahjulik mõju on väike.

6. Kasutusel olevad riskide vältimise meetmed

Kirjelda üldiselt, kuidas organisatsioonis tegeletakse riskide vältimisega. Kas sellega tegeleb konkreetne ametikoht jms.

6.1. Organisatsioonilised turvameetmed

Kirjelda, millised on organisatsioonis kasutusel olevad korralduslikud meetmed (näiteks protseduurid, korrad, juhendid ja sise-eeskirjad vms), et tagada füüsiliste isikute õiguste ja vabaduste kaitse.

6.2. Füüsilised turvameetmed

Kirjleda, millised füüsilised turvameetmeid (ligipääsuõigused jmt) rakendatakse, et tagada füüsiliste isikute õiguste ja vabaduste kaitse.

6.3. Infotehnoloogilised turvameetmed

Kirjelda, millised on organisatsioonis kasutusel olevad tehnilised meetmed (näiteks mingite konkreetsete andmete kaitsmiseks kasutatakse teatud krüptograafilist protokolli vms), et tagada füüsiliste isikute õiguste ja vabaduste kaitse.

Lisa 1

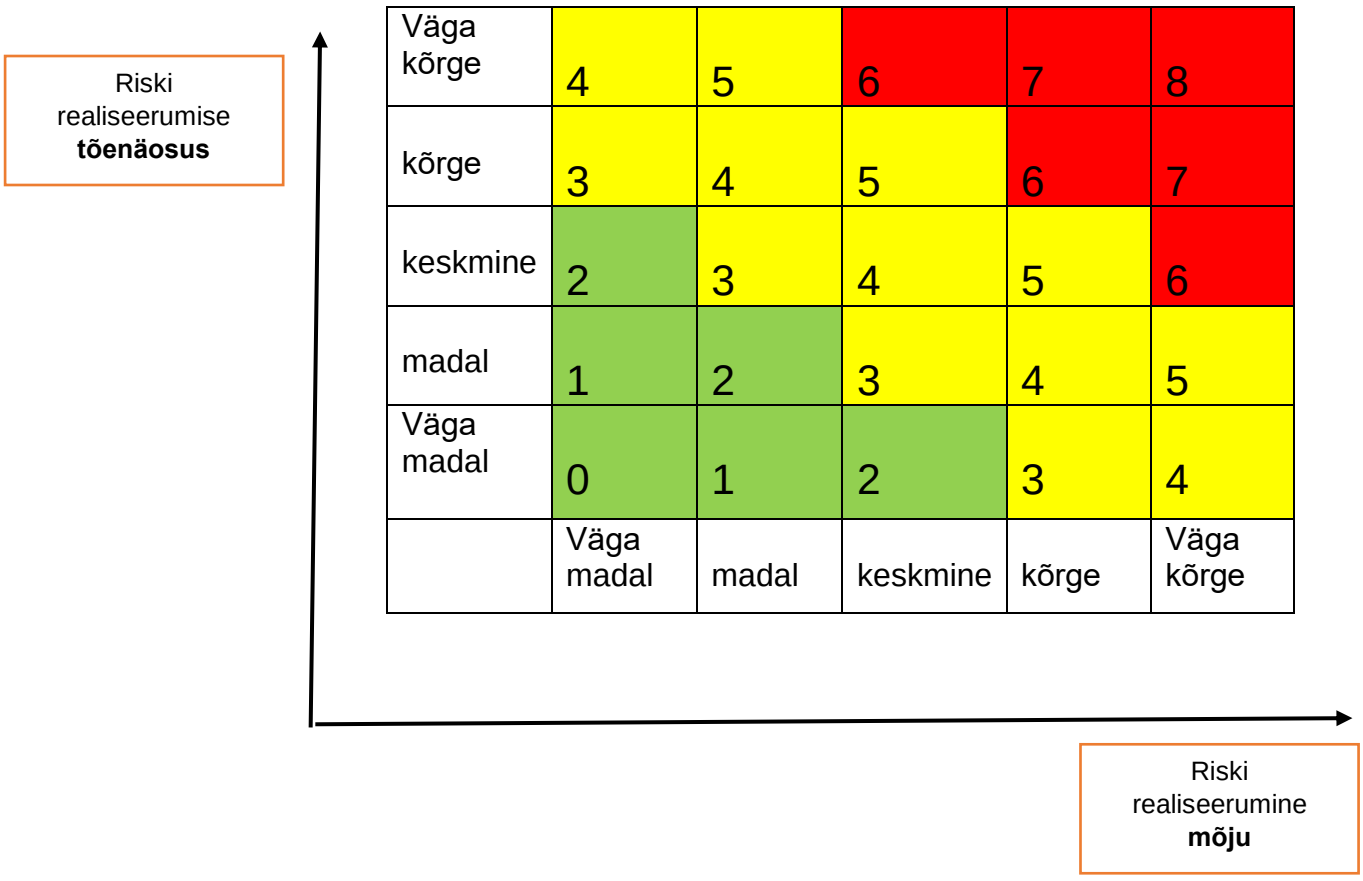
Riski hindamise näidis A

Riski hindamisel hinnatakse kahte tegurit skaalal 0-4:

- Riski realiseerumise **tõenäosus**
- Riski realiseerumise **mõju**

Üldine **riski tase** leitakse kahe skaala ristumispunktis.

Kui üldine riski tase on konkreetse riski/asjaolu kohta määratud, siis tuleb otsustada, mida riskiga ette võtte. Riski võib vältida, delegeerida/üle anda (transferred), vähendada või aktsepteerida.



Riski tase	
Tulemus	**Kirjeldus**
6-8	Kõrge
3-5	Keskmine
0-2	Madal

Lisa 2

Riski hindamise näidis B

Riski hindamisel hinnatakse kahte tegurit skaalal 1-5:

- Riski realiseerumise **tõenäosus**
- Riski realiseerumise **mõju**

Üldine **riski tase** leitakse kahe teguri korrutamisel.

Kui üldine riski tase on konkreetse riski/asjaolu kohta määratud, siis tuleb otsustada, mida riskiga ette võtte. Riski võib vältida, delegeerida/üle anda (transferred), vähendada või aktsepteerida.

Riski realiseerumise tõenäosus	
Tase	**Kirjeldus**
5	Peaaegu kindel
4	Tõenäoline
3	Võimalik
2	Ebatõenäoline
1	Harvaesinev

Riski realiseerumise mõju	
Tase	**Kirjeldus**
5	Katastroofiline
4	Suur
3	Mõõdukas, keskmine
2	Vähetähtis
1	Ebaoluline

Riski tase	
Tase	**Kirjeldus**
20+	Ekstreemne
11-19	Kõrge
5-10	Mõõdukas
1-4	Madal

Lisa 3

Allikad

Andmekaitsealase mõjuhinnangu koostamisel konsulteeriti või kasutati sisendi andjatena järgmisi allikaid:

- *Nimekiri allikatest*

Võtmeisikud käesoleva andmekaitsealase mõjuhinnangu kontekstis on:

- *Nimekiri võtmeisikutest*

Käesolevale andmekaitsealase mõjuhinnangule võib juurde panna täiendavaid lisasid (näiteks organisatsiooni andmekaitse kord, andmekaitse spetsialisti ametijuhend vms).