



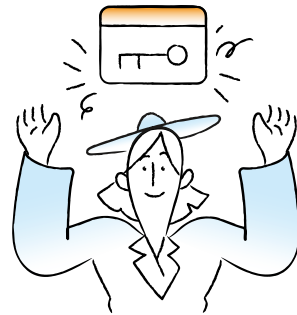
MÕJUHINNANG

Mis on mõjuhindang?

2018. aasta 25. maist kohaldatakse Euroopa Liidus isikuandmete kaitse üldmäärust (IKÜM), kus on võetud kasutusele andmekaitsealase mõjuhindangu mõiste.

Mõjuhindang kirjeldab, kuidas ettevõttes isikuandmeid töödeldakse ning milliseid meetmeid isikuandmete kaitsmiseks rakendatakse. Mõjuhindangut võib võrrelda ettevõtetele tuttava riskianalüüsiga, kuid see hindab kitsalt isikuandmete töötlemist ning sellel lasuvaid riske inimese vaatest.

Mõjuhindangu eesmärk on tuvastada, kas isikuandmete kaitseks rakendatavad meetmed on piisavad, et tõenäoliselt ohte kas täielikult maandada või vähemalt vastuvõetavale tasemele leevendada.



Kes peavad mõjuhindangu tegema?

Mõjuhindangu peavad tegema isikuandmete töötlemise eest vastutavad andmetöötledajad, kelle isikuandmete töötlemise laadi, ulatust, konteksti ja eesmarke arvestades tekib inimesele tõenäoliselt suur oht. Töötlemise ulatuslikkuse ja süsteemsuse määramisel tuleb ettevõttel lähtuda kindlatest kriteeriumidest.

Eestis on siseriikliku mõjuhindangu ulatuslikkuse kriteeriumid järgnevad:

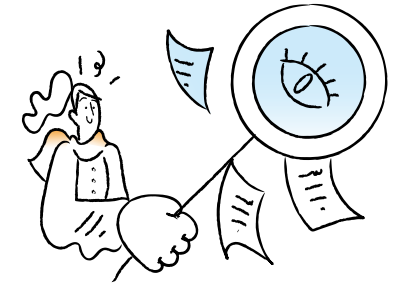
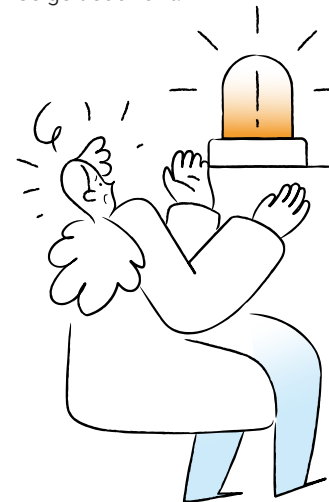
- eriliiki andmed või süüteoandmed 5000 ja enama inimese kohta;
- suurt ohtu põhjustavad andmed 10 000 ja enama inimese kohta;
- ülejäänud isikuandmed 50 000 ja enama inimese kohta.

Mis on (suur) oht?

Oht hõlmab sündmust ja selle tagajärgi ning seda hinnatakse mõju, tõenäosuse ja inimese perspektiivist.

Suur oht isikuandmetega seotud rikkumise mõttes on eelkõige oht inimese elule, tervisele, varale ja mainele.

Suure ohu ja lihtsalt ohu eristamine sõltub tagajärje raskusest. Lihtsamaks ohuks on näiteks infosüsteemi tõrge, mis ei lase e-poe teenuseid kasutada ega kliendil ostuajalugu vaadata. Perearstikeskuse infosüsteemi tõrge seevastu on ilmselgelt suur oht.



Kõrge riskiga andmetöötlus, mis vajab mõjuhindangu koostamist, võib olla näiteks:

- innovaatilise tehnoloogia kasutuselevõtmine isikuandmete töötlemisel;
- inimese asukoha või käitumise jälgimine;
- geneetiliste või biomeetriliste andmete töötlemine;
- kaupade või teenuste turundamine haavatavatele sihtgruppidele (näiteks alaealised või vanemaealised).

Mõjuhindangu miinimumnõuded on, et isikuandmete töötlemise eest vastutav ettevõtte hindaks ja kirjeldaks:

- a) milliseid isikuandmeid ning millisel eesmärgil ettevõtte töötleb;
- b) millisel õiguslikul alusel ettevõtte isikuandmeid töötleb;
- c) milliseid meetodeid ettevõtte isikuandmete töötlemisel kasutab;
- d) kuidas töötlemiseks kavandatud valikud on eesmärgi saavutamiseks vajalikud ja kohased;
- e) millised on võimalikud ohud ja ohtasemed (nt kõrge, keskmine, madal);
- f) milliseid tagatise ja meetmeid ettevõtte ohtude vastu rakendab.

Kas olen hinnanud mõjuhinnangu koostamise vajadust ettevõttes?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Kui isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärgi arvestades tekib tõenäoliselt <u>suur oht inimesele</u>, siis tuleb teha mõjuhinnang. - Mõjuhinnang on käepärane tööriist võimalike riskide minimeerimiseks, mistõttu on soovitatav see organisatsioonis läbi viia rohkematele töötlusprotsessidele kui seadusandlus otseselt kohustab. Hindamine aitab võimalikke kitsaskohti tuvastada ja maandada.
Kas olen koostanud kirjaliku mõjuhinnangu?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Kuna puudub kindel ülesehituslik suunis, on igal ettevõttel võimalik koostada oma vajadusi arvestav kirjalik hindamine. - Hindamine on ettevõttele oluliseks töövahendiks, mistõttu tasub selle koostamisel eelkõige enda vastu aus olla, tegelikku olukorda peegeldada ning tegelikult tekkivaid riske hinnata.
Kas olen koostanud isikuandmete töötlemise kirjelduse?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Kirjeldatakse töödeldavaid isikuandmeid, nende saajaid ja andmete säilitustähtaegu. - Kaardistatakse, kes või mis andmetöötluses osalevad (töötajad, riist- ja tarkvara, andmesideseadmed, andmekandjad).
Kas olen hinnanud isikuandmete töötlemise vajalikkust ja proportsionaalsust ning kavandanud meetmed isikuandmete kaitsmiseks?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Kirjeldatakse isikuandmete kogumise selgelt kindlaks määratud ning õiguspäraseid eesmärgi ja seadusest tulenevaid aluseid. - Töödeldakse ainult neid andmeid, mis on vajalikud eesmärkide täitmiseks. - Märgitakse, kui kaua andmeid säilitatakse, st andmeid säilitatakse ainult seni, kuni see on eesmärkide täitmiseks vajalik. <p>Kaitsemeetmed võivad olla kõik meetmed alates täiustatud tehniliste lahenduste kasutamisest kuni personali koolituseni. Olenevalt kontekstist ja isikuandmete töötlemisega seotud riskidest võivad sobivad meetmed olla alljärgnevad:</p> <p>1) isikuandmete pseudonümiseerimine, 2) töötajate koolitamine, 3) volitatud töötajate kohustamine lepinguliselt järgimaks andmetöötlemise põhimõtteid, 4) säilitustähtaegade kohta info jagamine, 5) inimestele töötlemisse sekkumise võimaldamine, 6) struktureeritud säilitamine jne.</p> <p>Kaitsemeetmetest leiab informatsiooni <u>EU suunistest</u>.</p>
Kas olen hinnanud isikuandmete töötlemisega kaasnevat võimalikke ohte?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Mõjuhinnang eeldab riskil põhineva meetodi kasutamist – kaardistada riskid ja neid hinnata. Hinnata tuleks riski realiseerumise tõenäosust ja võimalikke tagajärgi. - Arvestada tuleb ohu päritolu, allikaid, laadi, eripära, tõenäosust ja mõju andmete käideldavusele, terviklusele ja konfidentsiaalsusele. - Hinnata tuleb ohu realiseerumisel inimesele tekkivat võimalikku füüsilist, varalist või mittevaralist kahju (nt maine kahju, rahaline kahju, identiteedivargus või -pettus, diskrimineerimine). Teisisõnu, määratakse inimesele tekkiva tõenäolise ohu (kahju) tase. - Valitakse turvameetmed riskide haldamiseks ning otsustatakse, kas aktsepteeritakse jääkriski.
Kas olen kaasanud isikuandmete töötlemisel olulisi inimesi?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Mõjuhinnangu koostamisse on kaasatud asjassepuutuvad pädevad inimesed ning <u>andmekaitse spetsialist</u> (kui on ettevõttes).
Kas olen järginud ajakohasuse, konkreetsuse ja loogilisuse põhimõtteid?	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> - Mõjuhinnang on elav dokument ning käib käsikäes ettevõtte muutustega seoses isikuandmete töötlemisega (näiteks on töötlemise eesmärgid muutunud, andmetöötlemise käigus ilmnevad uued suured ohud jne). - Sarnaseid suurt ohtu kujutavaid andmetöötlemiseid võib hinnata koos. Kooshindamist võiks teha ka siis, kui andmetöötlemise on kaasatud mitu andmetöötajat. Eriti oluline on sel juhul täpselt fikseerida vastutus kaitsemeetmete ees. Näiteks võib tuua kaupluste ja turvaettevõtte koostöö kaameravalve kasutamise mõjuhinnangu tegemisel.

* Mõjuhinnangu vastavuse hindamiseks saate kasutada kontrollnimekirja. Kui vastate kõikidele küsimustele jaatavalt, siis vastab mõjuhinnang eelduslikult tingimustele. Kui vastus mõnele küsimusele on eitav, siis tuleb ettevõttel veelkord oma tegevused läbi mõelda.