ANDMEKAITSE INSPEKTSIOON

ISIKUANDMETE TÖÖTLEJA ÜLDJUHEND

Kinnitatud 31.05.2018

Muudetud 28.09.2018

Muudetud 19.03.2019

Üldjuhend võtab kokku kõige olulisema, mida isikuandmete töötleja peab teadma.

Üldjuhend on suunatud kõigile sektoritele ega sisalda soovitusi kitsamatele tegevusvaldkondadele.

Sisukord

Sissejuhatus ja põhimõisted

Miks on vaja reegleid isikuandmete töötlemise kohta? Sest inimesed vajavad kindlustunnet, et nende kohta käivat teavet kogutakse ja kasutatakse ausalt, õigesti ja turvaliselt. Ilma selleta ei teki usaldust. Kui inimesed ei usalda, kuidas nende andmeid kasutatakse, siis digimajanduse ja e-riigi areng seiskub.

Aga arengut takistab ka ülereguleerimine ja juriidiline ülemõtlemine. Kahjuks kasutatakse andmekaitset nii mõnigi kord vabanduseks laiskusele ja lollusele. Andmekaitse eesmärk ei ole öelda, et mitte midagi ei tohi teha, vaid kuidas saab vajalikke asju õigesti teha.

Andmekaitsereeglite mõistlik tõlgendamine, kavakindel järgimine ning tõhus infoturve aitavad tagada inimeste usaldust ning ühtlasi kaitsta ettevõtte/asutuse (info)vara.

Eesti põhiseadus kaitseb pere- ja eraelu puutumatust, sõnumisaladust, õigust vabale eneseteostusele ning annab õiguse küsida avaliku sektori asutustelt teavet, mida neil küsija kohta on. Kogumis loovad nad aluse isikuandmete kaitsele.

Euroopa Liidu ja Eesti andmekaitseõigus uueneb. Alates 25. maist 2018 rakendatakse isikuandmete kaitse üldmäärust 2016/679 (edaspidi ***üldmäärus***).[1] Maikuus tuli üle võtta õiguskaitseasutuste andmekaitsedirektiiv 2016/680 (edaspidi ***direktiiv***).[2] Käesolev üldjuhend võtab kokku kõige olulisema, mida isikuandmete töötleja peaks neist teadma.

Üldjuhend on – nagu nimigi ütleb – üldine selgituste kogumik. Ta on suunatud kõigile isikuandmete töötlejatele – ettevõtetele, mittetulundusühingutele, asutustele, ametiisikutele. Üldjuhendis ei ole kitsamatele valdkondadele suunatud soovitusi.

Seetõttu pöördun ettevõtlus-, kutse- ja erialaliitude poole. Kindlasti on teie tegevusvaldkonnas probleeme, mida üldjuhend ei käsitle. Keegi ei tunne neid paremini ega oska paremaid lahendusi pakkuda kui te ise. Inspektsiooni võimalused anda üksikutele andmetöötlejatele põhjalikumat nõu on kasinad. Kuid oleme rõõmuga valmis aitama, kui panete pead kokku ning asute ühiselt koostama oma kutse- või eriala jaoks hea tava toimimisjuhendeid, meelespäid, dokumendipõhjasid, sertifitseerimisskeeme ja muid abimaterjale.

Üldjuhend ei ole oma sisult uus dokument. Ta tugineb 2017. a. mais ja juunis inspektsiooni võrgulehel avaldatud teemaartiklitele ning 2018. a. 25. mail ülekinnitatud Euroopa andmekaitseasutuste ühisseisukohtadele.[3]

---

[1] Üldmääruse ametlik pealkiri on: *„Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)“*. Üldmäärus on avaldatud Euroopa Liidu Teatajas L 119, 04.05.2016, lk 1-88.

[2] *„Õiguskaitseasutuste andmekaitsedirektiiv“* ei ole ametlik nimi, vaid katse leida eesti keeles arusaadavat lühivarianti. Direktiivi ametlik pealkiri on: *„Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK“*. Direktiiv on avaldatud Euroopa Liidu Teatajas L 119, 04.05.2016, lk 89-131.

[3] Käesolevas üldjuhendis on kasutatud järgmisi 2018. a. 25. mail ülekinnitatud Euroopa andmekaitsenõukogu suuniseid: Suunised andmekaitseametnike kohta; Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679; Suunised, mis käsitlevad isikuandmetega seotud rikkumistest teatamis määruse 2016/679 alusel; Suunised andmete ülekandmise õiguse kohta; Suunised määruse (EL) 2016/679 kohase nõusoleku kohta; Suunised määruse 2016/679 kohase *läbipaistvuse kohta*.

Kuna riigisiseseid rakendusakte üldjuhendis esmase koostamise ajal polnud, siis kommenteerime üldmääruse kõrval direktiivi sisu (kuigi direktiiv ei ole otsekohalduv) ning lisame ka asjakohased viited isikuandmete kaitse seaduse (IKS) sätetele, mis võtavad direktiivi üle.

Üldjuhendi põhikoostajad on inspektsiooni tehnoloogiadirektor Urmo Parm ja koostöödirektor Maarja Kirss ülejäänud kolleegide aktiivsel osalusel. Üldjuhendi algmaterjal (teemaartiklid) on esitatud arvamuse avaldamiseks inspektsiooni nõukojale ning paljudele riigiasutustele, kutse- ja erialaühendustele. Tänan kõiki, kes panustasid. Loomulikult on tegemist „elava" dokumendiga, mille asja- ja ajakohastamine jätkub.

Üldjuhend lähtub väljakujunenud eesti õiguskeelest. Kutsun kõiki üles kasutama andmekaitse alal head eesti keelt, näiteks:

- isikuandmete kaitse üldmäärus (IKÜM) või lihtsalt (andmekaitse) üldmäärus, mitte ~~General Data Protection Regulation (GDPR)~~,
- andmekaitsespetsialist (AKS), mitte ~~*data protection officer* (DPO)~~,[4]
- andmekaitsetingimused, mitte ~~privaatsuspoliitika~~,[5]
- isikuandmete töötlemisülevaade, mitte ~~isikuandmete töötlemise toimingute register.~~[6]

Enne sisupeatükke soovitan tutvuda mõistete[7] lühikursusega:

Asjad, mida teadmata ei saa järgnevaist peatükkidest aru

Isikuandmed on teave inimese ehk füüsilise isiku (**andmesubjekti**) kohta, millega teda saab otse või kaude tuvastada: nimi, isikukood, asukohateave, võrguidentifikaatorid (tunnused, mis sidevõrgus aitavad viia konkreetse isikuni), samuti füüsilised, geneetilised, vaimsed, majanduslikud, kultuurilised ja mistahes muud tuvastamist võimaldavad tunnused ja nende kombinatsioonid.[8]

Näide A: mingis nimekirjas olev ainsa Jaan Tamme puhul piisab otseseks tuvastamiseks tema nimest.
Näide B: kui nimekirjas on kõik Eestis elavad Jaan Tammed, siis nimest üksi ei piisa, kuid koos isikukoodi ja/või koduse aadressiga on isik selgesti eristatav nimekaimudest ning otseselt tuvastatav.
Näide C: tuvastamine võib olla kaudne, eri andmetest kombineeritud – räägitakse nime nimetamata ettevõtjast, kes on üks Tallinnas asuva osaühingu N.N. viiest osanikust ning ühtlasi Tartumaal paikneva talukoha omanik. Igaüks saab äriregistrist tuvastada, kes need viis osanikku on, ning siis leida kinnistusraamatust, et neist vaid Jaan Tammel on Tartumaal talu.

Eriliiki isikuandmed on andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, isiku

[4] Üldmääruse eestikeelne versioon kasutab ebaõnnestunud terminit ***andmekaitseametnik***, mis ei sobi kasutamiseks väljaspool avalikku teenistust riigi ja omavalitsuste ametiasutustes. Üldmääruse artiklis 39 nimetatud ülesanded on oma sisult spetsialisti-taseme ülesanded. See, kas andmekaitsespetsialistil on veel mingeid muid ülesandeid, mis võimaldavad teda nimetada näiteks ettevõtte ***andmekaitsejuhiks***, on ettevõtte-sisene suhe. Välispidiselt tuleb igal juhul kasutada ***andmekaitsespetsialisti*** nimetust.

[5] Üldmääruse art. 12 lõikes 1 nimetatud teave tervikdokumendina. Termin lähtub sellest, et see on ettevõtte üld- või tüüptingimuste laadne dokument või lausa selle üks osa.

[6] Üldmääruse art. 30 on pealkirjastatud eksitavalt ***Isikuandmete töötlemise toimingute registreerimine,*** direktiivi art. 24 analoogse normi pealkiri on ***Isikuandmete töötlemise toimingute dokumenteerimine*** ning IKS § 37 pealkiri on ***Isikuandmete töötlemise toimingute registreerimine***. Tegelikult peetakse siin silmas ettevõtte/asutuse-sisest isikuandmete töötlemise ülevaate koostamist, mitte logiraamatu-laadset toimingute registri pidamist. Mõistlik on nimetada asja sellena, mis ta on.

[7] Direktiiv võeti üle isikuandmete kaitse seaduse 4. peatükiga. Selle peatüki üks säte, § 13, määratleb, et selle peatüki tähenduses kasutatakse termineid üldmääruse art. 4 ning art 9 lõike 1 tähenduses. Samas paragrahvis määratletakse ka ära õiguskaitseasutuse mõiste.

[8] Vt üldmääruse art. 4 p.1; direktiivi art. 3 p. 1.

kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed ja andmeid seksuaalelu ja seksuaalse sättumuse kohta.[9]

Isikuandmete töötlemine on andmetega tehtav mistahes toiming: kogumine, korrastamine, säilitamine, muutmine, lugemine, kasutamine, edastamine, ühendamine, kustutamine jne.[10]

Isikuandmete kaitse reeglid <u>ei kehti</u>, kui:

1) tegu on juriidilise isiku või asutuse andmetega;[11]
2) teave ei võimalda inimest mõistlike pingutustega tuvastada;[12]

Näide A: üks eraisik ei tea reeglina teise eraisiku arvuti IP-aadressi või muud võrguidentifikaatorit, seevastu sideettevõte tunneb nende järgi oma kliendid ära.
Näide B: fail patsientide terviseandmetega on kas krüpteeritud või on nimed asendatud kas varjunimede või suvaliste numbritega. Sellele, kes saab faili lahti krüpteerida või kes oskab varjunimesid pärisnimedega asendada, on tegu isikuandmetega. Sellele, kes ei saa seda teha, ei ole tegu isikuandmetega.
Näide C: erinevalt e-posti aadressist eesnimi.perenimi@ettevõttenimi.ee ei sisalda aadress myygimees@ettevõttenimi.ee võõraste jaoks isikuandmeid. Kui aga ettevõtte sees on teada, et seda aadressi saab kasutada vaid üks konkreetne töötaja, siis teadjate jaoks on tegu isikuandega.

3) isikuandmeid ei töödelda automatiseeritult ning neist ei tehta ka andmekogumit;[13]

Näide A: patsientide nimekirja peetakse arvutifailis – see tähendab automatiseeritud andmetöötlust, seega isikuandmete kaitse reeglid kehtivad.
Näide B: õpilaste nimed ja õpitulemused märgitakse paberkausta, nimed on järjestatud tähestikuliselt ning õpitulemused märgitud nimede juurde ajalises järjestuses. Automatiseeritud andmetöötlust ei ole, kuid tegu on korrastatud andmekogumiga, seega isikuandmete kaitse reeglid kehtivad.
Näide C: nimesid ja äratuntavaid näokujutisi sisaldav graffiti majaseintel ei ole automatiseeritud andmetöötlus ega ka andmekogum, seega isikuandmete kaitse reeglid ei kehti. Inimene, keda graffiti sisu kahjustab (näiteks teotab tema au ja head nime), saab esitada nõudeid võlaõigusseadusele, mitte isikuandmete kaitse üldmäärusele tuginedes.
Näide D: elulooraamat kajastab nii peategelase kui paljude teiste reaalseid eluloosündmusi. Automatiseeritud andmetöötlust pole, kuid tegemist on andmete kogumisega, seega isikuandmete kaitse reeglid kehtivad.
Näide E: sideettevõtte väljaantud telefoniraamat (paberil) eraisikute nimede ja telefoninumbritega on selgesti andmekogum, isikuandmete kaitse reeglid kehtivad.

4) isikuandmeid kasutatakse isiklikul otstarbel või kodumajapidamise tarvis;[14]

Näide A: inimese isiklik telefoniraamat tuttavate kohta – olgu pabermärkmikuna või arvutis – on isiklikul eesmärgil andmetöötlus, isikuandmete kaitse reeglid ei kehti.
Näide B: sugulaste nimekiri suguvõsa kokkutuleku korraldamiseks on mitme inimese isiklikul eesmärgil toimuv andmetöötlus senikaua, kuni see on suguvõsa-siseses kasutuses. Kui nimekirja hakatakse jagama ettevõtetega ja kasutama näiteks ärilise reklaami saatmiseks, siis ei ole enam tegu isikliku otstarbega.
Näide C: sama kehtib arutelu kohta suhtlusvõrgustiku rühmas, mille liikmeks on eraisikud. See on mitme inimese isiklikul eesmärgil toimuv andmetöötlus, isikuandmete kaitse reeglid ei kehti. Kui

[9] Vt üldmääruse art. 9 ja direktiivi art. 10. See mõiste on kattuv seni Eesti õiguses kasutatud ***delikaatsete isikuandmete*** mõistega – välja arvatud selles osas, et eriliiki isikuandmed ei hõlma süüteoandmeid ja süüdimõistvaid kohtuotsuseid (vt üldmääruse art. 10).
[10] Vt üldmääruse art. 4 p. 2; direktiivi art. 3 p. 2.
[11] Vt üldmääruse art. 1; direktiivi art. 1.
[12] Vt üldmääruse sissejuhatuse põhjenduspunkt (edaspidi ***pp***.) 26 ja 57 ning art. 11; direktiivi pp. 21.
[13] Vt üldmääruse art. 2 lg 1; direktiivi art. 2 lg 2.
[14] Vt üldmääruse art. 1 lg 2 p. c.

rühmaga liituvad ettevõtted või kui suhtlus on rühmaliikmete ameti- või äritegevuse osaks, siis ei ole enam tegu isikliku otstarbega ning isikuandmete kaitse reeglid kehtivad.

5) liikmesriik kasutab isikuandmeid oma julgeoleku tagamiseks või Euroopa Liidu ühise välis- ja julgeolekupoliitika raames.[15]

Õigus isikuandmete kaitsele ei kehti piiramatult. Ta ei ole iseenesest rohkem ega vähem tähtsam kui teised põhiõigused. Ühe inimese õigus eraelule võib põrkuda teise inimese sõna- ja teabevabadusega, eneseteostusvabadusega, ettevõtlusvabadusega. Põhiõigusi tuleb konkreetses olukorras omavahel kaaluda. Avalikus sektoris võib eraelu piirata avaliku huvi kaalutlustel. Teatud küsimustes on seadusandja andnud täpsemad kaalumisreeglid – näiteks ajakirjanduslikult eesmärgil isikuandmete töötlemiseks.[16]

Isikuandmete töötlemise peamised põhimõtted on:[17]

1) seaduslikkus – igasuguseks isikuandmete töötlemiseks peab olema alus;
2) eesmärgipärasus – määratle eesmärk, milleks andmeid vajad. Samade andmete muu eesmärgil töötlemiseks peab olema teine alus;
3) minimaalsus – tuleneb eesmärgist: ära kogu rohkem andmeid kui eesmärgi saavutamiseks vaja on;
4) õigsus ehk andmekvaliteet – tuleneb samuti eesmärgist: andmed olgu eesmärgi saavutamiseks asja- ja ajakohased;
5) säilitamistähtaeg – eesmärgist tuleneb ka säilitamistähtaeg;
6) turvalisus – hoia ja töötle andmeid turvaliselt,
7) vastutus ja läbipaistvus – andmetöötleja vastutab nende põhimõtete järgimise eest ning peab olema andmesubjekti jaoks läbipaistev (andma teavet, võimaldama tutvuda ja nõudeid esitada).

Isikuandmete töötlemise alused:[18]

1) nõusolek – nõusoleku olemasolu peab tõendama andmetöötleja. Nõusolek on ühepoolselt tagasivõetav.

Näide A: nõusolek peab olema informeeritud – inimene peab teadma, milleks täpselt (mis eesmärgiks ta nõusoleku annab). Nõusolekut ei saa võtta lihtsalt andmetöötluseks.
Näide B: nõusolek peab olema vabatahtlik – seda ei saa kokku siduda muude tingimustega (Sa ei saa meie ettevõtte kliendiks hakata ja lepingut sõlmida, kui Sa ühtlasi ei anna nõusolekut edaspidi meilt reklaami saamiseks).
Näide C: ettevõtted/asutused kipuvad lepingu või avaliku ülesande alusel toimuva andmetöötluse korral lisama täiendava alusena nõusolekut. Nõusolek on ühepoolselt tagasivõetav. Ei saa nii olla, et kui inimene nõusoleku tagasi võtab, siis teatatakse, et seesama andmetöötlus jätkub nüüd lepingu alusel või avaliku ülesande täitmiseks. Kui inimeselt võetakse nõusoleku laadne kinnitus tema kohta käiva andmetöötluse kohta ja tal ei ole võimalik sellest andmetöötlusest kas kohe või hiljem keelduda, siis on tegu eksliku, algusest peale kehtetu nõusolekuga. Muu alus (nt. leping) võib aga sealjuures ikkagi kehtida.

2) leping – lepingu sõlmimiseks või sõlmitud lepingu täitmiseks vajalik andmetöötlus.

Isikuandmete töötlemiseks ei ole vaja sõlmida eraldi lisa-lepingut, kui see on juba kaetud põhilepinguga (nt töölepinguga). Lepingusse ei ole vaja lisada tühisätteid, mis nendivad, et lepingu täitmiseks võib ettevõte oma kliendi/töötaja andmeid töödelda;

3) seadusejärgne kohustus – näiteks ettevõtte/asutuse kohustused, mis tulenevad raamatupidamis- või maksuseadustest;

[15] Vt üldmääruse art. 2 lg 2 p. a ja b; direktiivi art. 2 lg 3 p. a.
[16] Vt eelkõige üldmääruse pp. 4 ning lisaks pp. 153-159 ning art. 85, 86, 88, 89. Lisaks vt IKS § 4.
[17] Vt üldmääruse art. 5; direktiivi art. 4; IKS § 14.
[18] Vt üldmääruse art. 6, täiendavad nõuded eriliiki andmete osas art. 9, vt samuti art. 7-11; direktiivi art. 8; IKS § 15.

4) avaliku võimu teostamine, avaliku ülesande täitmine – andmetöötlus võib olla õigusaktis otse nimetatud või ka tuletatud selle täitmise vajadusest;
5) inimese eluliste huvide kaitseks, et teda hädas aidata (näiteks on inimene kontaktivõimetu või kadunud);

> *Inimeste eluliste huvide kaitsele saab viidata erandlikus olukorras, mitte siis, kui tegu seadusejärgse kohustusega (nt. lastekaitseseadus kohustab igaüht hädasolevast lapsest pädevale asutusele teatama) või avaliku ülesande täitmise või avaliku võimu teostamisega (millele tuginevad riigi ja omavalitsuse asutused ja ametiisikud, nt politseinikud ja sotsiaaltöötajad).*

6) selline õigustatud huvi, mis kaalub üles inimese õiguse eraelule ja isikuandmete kaitsele.

> *Õigustatud huvi on samuti erandlik ning peaaegu alati vaieldav andmetöötluse alus. Seda tasakaalustab nõue, et inimesele tuleb tema kohta käivast andmetöötlusest teada anda (vt üldmääruse art. 13 ja 14).*

Isikuandmete vastutav töötleja on see ettevõte/asutus, kes määrab kindlaks isikuandmete töötluse eesmärgid ja vahendid. **Volitatud töötleja** on see, kes vastutava töötleja nimel ja ülesandel isikuandmeid töötleb. **Vastuvõtja** on iga isik või asutus, kellele isikuandmeid avaldatakse.[19]

> *Näide: ettevõte/asutus tellib avaliku arvamuse uuringu, püstitades uuringu eesmärgid ja andes selleks raha. Tellijana on ta vastutav töötleja. Uuringufirma, kes tema tellimusel inimesi küsitleb ning tulemused kokku võtab, on volitatud töötleja. Andmemajutusettevõte, kes hiljem uuringu andmestikku oma serveris säilitab, on samuti volitatud töötleja. Vastutav ja volitatud töötleja on selles näites ettevõtted. Nende töötajad (nt küsitlejad uuringufirmas) ei ole ise vastutavad/volitatud töötlejad. Kuid nii uuringufirma, andmemajutusettevõte kui ka nende töötajad on kõik isikuandmete vastuvõtjad.*

Viljar Peep,
üldjuhendi toimetaja

[19] Vt üldmääruse art. 4 p. 8 ja 9 ning art. 24, 26, 28 ja 29; direktiivi art. 3 p. 8 ja 9 ning art. 19, 21-23; IKS § 29-32.

1. peatükk. Andmetöötleja peamiste kohustuste nimekiri

Kohustus	Kirjeldus
Isikuandmete töötlemise põhimõtete rakendamine	Andmetöötleja lähtub andmete töötlemisel: - seaduslikkuse, õigluse ja läbipaistvuse põhimõttest - eesmärgi piirangu põhimõttest - võimalikult väheste andmete kogumise põhimõttest - õigsuse ehk andmekvaliteedi põhimõttest - säilitamise piirangu põhimõttest - usaldusväärsuse (konfidentsiaalsuse) põhimõttest - vastutuse põhimõttest
Turvaline isikuandmete töötlemine	Andmetöötleja rakendab andmetele vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslike meetmeid.
Andmekaitsespetsialist	Andmetöötleja määrab andmekaitsespetsialisti, kui ta: - on avaliku sektori asutus või organ, sh avalikke ülesandeid täitev eraõiguslik isik; - põhitegevuseks on inimeste ulatuslik korrapärane ja süstemaatiline jälgimine; - põhitegevuseks on eriliiki isikuandmete või süüteo-andmete ulatuslik töötlemine. Andmetöötleja teeb avalikult kättesaadavaks andmekaitsespetsialisti kontaktandmed ja esitab need ka andmekaitseasutusele. Eestis saab mõlemat korraga teha äriregistri kaudu
Andmekaitsetingimuste avaldamine	Vastutav töötleja annab inimesele teavet tema andmete töötlemise tingimuste kohta
Lõimitud ja vaikimisi andmekaitse rakendamine	Uute toodete/ teenuste või isikuandmeid mõjutava töökorraldusmuudatuse kavandamise ning rakendamise käigus tuleb algusest peale arvestada andmekaitse põhimõtete ning asjakohaste turvameetmete rakendamisega. Vaikevalikud (algseadistused) peavad võimalikest valikutest olema kõige privaatsussõbralikumad
Isikuandmete töötlemisülevaade	Vastutavad ja volitatud töötlejad peavad koostama isikuandmete töötlemisülevaate. Nõue kehtib kõigi andmetöötlejate kohta (v.a. organisatsioon, kellel pole töötajaid ega füüsilisest isikust kliente)
Rikkumisteated	1. Vastutav töötleja dokumenteerib kõik isikuandmetega seotud rikkumised, sh asjaolud, mõju ja parandusmeetmed. 2. Vastutav töötleja teavitab isikuandmetega seotud rikkumisest andmekaitseasutust 72 tunni jooksul (v.a. juhul, kui rikkumine ei kujuta inimesele ohtu). 3. Vastutav töötleja teavitab viivitamatult inimesele tema andmetega seotud rikkumisest, kui see kujutab endast suurt ohtu (v.a. juhul, kui andmed on muudetud loetamatuks või võetud muud kahju leevendavad meetmed või kui teavitamine nõuab ebamõistlikke pingutusi – viimasel juhul asendatakse isiku teavitamine avaliku teadaandega)

Mõjuhinnang	Vastutav töötleja hindab ja dokumenteerib enne tõenäoliselt suurt ohtu põhjustava andmetöötlusega alustamist selle mõju ning enda tegevuse. Iseäranis on suure ohuga tegemist, kui: 1) toimub süsteemne ulatuslik automatiseeritud hindamine/profileerimine, millel on inimese jaoks õiguslikud tagajärjed või oluline mõju; 2) eriliiki või süüteoandmeid töödeldakse ulatuslikult; 3) avalikke alasid jälgitakse ulatuslikult
Eelnev konsulteerimine	Vastutav töötleja peab konsulteerima enne andmetöötlusega alustamist andmekaitse järelevalveasutusega juhul, kui mõjuhinnangust selgub, et hoolimata meetmete rakendamisest jääb suur oht isiku õigustele ja vabadustele püsima
Isikuandmete ülekandmine	Inimene võib nõuda vastutavalt töötlejalt nõusolekul või lepingul põhineva automatiseeritud andmetöötluse korral teda puudutavate andmete, mida ta ise on esitanud, masinloetavat üleandmist teisele ettevõttele
Kolmandatesse riikidesse edastamise nõuded	Andmete edastamisel väljapoole Euroopa majanduspiirkonda tuleb jälgida, kas tegemist on piisava või mittepiisava andmekaitsetasemega riigiga [20] Piisava andmekaitsetasemega kolmandate riikide nimekiri on Euroopa Komisjoni võrgulehel. Mittepiisava andmekaitsetasemega kolmandasse riiki isikuandmed edastades tuleb rakendada üldmääruse artikli 46 kohaseid kaitsemeetmeid. Üldmääruse artikkel 49 reguleerib erandjuhtumid, mil võib isikuandmeid kolmandasse riiki edastada ilma vastavaid kaitsemeetmeid rakendamata. Õiguskaitseasutuste andmekaitsedirektiivi kohased isikuandmete edastamise nõuded on toodud IKS §-des 46-50. Kolmandatesse riikidesse edastamise lähemaid reegleid käesolevas üldjuhendis ei käsitleta. See info on Euroopa Komisjoni võrgulehel, samuti Euroopa andmekaitsenõukogu võrgulehel

[20] Euroopa majanduspiirkond on Euroopa Liit ning Island, Norra ja Liechtenstein.

2. peatükk. Lõimitud ja vaikimisi andmekaitse. Logid

Vt üldmääruse art. 25 ja pp. 78; direktiivi art. 20 ja pp. 53; IKS § 33.

Üldmäärus ja direktiiv (need normid on üle võetud IKS-i) sätestavad andmetöötleja vastutuse põhimõtte. Andmetöötleja peab jälgima niihästi õigusnorme ja õiguspraktikat kui ka infotehnilist arengut, sellest tulenevaid võimalusi ja ohte. Kuid norme rakendavad ja tehnoloogiat kasutavad ikkagi inimesed. Andmeid töötleva ettevõtte/asutuse töökorraldus on kõige alus.

Üldmäärus ja direktiiv annavad esmakordselt lõimitud- ja vaikimisi andmekaitsele õiguslikult siduva tähenduse. Tegu ei ole siiski uute mõistetega andmekaitsepraktikas. Mõlemad käsitlused on omavahel seotud. Seetõttu tuleks neid rakendada koos, vastastikku toetavalt.

Mis on lõimitud andmekaitse?

Lõimitud andmekaitse põhimõtted töötati välja juba 1990. aastatel. Need olid ja on suunatud infotehnoloogia ning mahukate andmetöötlussüsteemide üha suurenevale mõjule inimeste privaatsusele.

Läbiv vaatenurk on, et eraelu kaitset ei saa tagada ainult õigusnormistikule vastavuse abil, vaid see peab tulenema organisatsiooni töökorraldusest ning infotehnoloogiast. Mida tundlikumad andmed, seda tõhusam peab olema kaitse. Lõimitud andmekaitse ei ole mitte niivõrd õiguslik mõiste, kuivõrd mõtteviis ja organisatsioonikultuur.

Järgnevad põhimõtted kirjeldavad lõimitud andmekaitse rakendamist:

1) **enneta, mitte ära tegele tagajärgedega**

Ohte tuleb ette näha ja ära hoida enne nende toimumist. Andmekaitse on organisatsiooni tegevusse ning tema infosüsteemidesse sisse ehitatud enne isikuandmete töötlemisega alustamist;

2) **andmekaitse korrapärasus ja süsteemsus**

Andmekaitse on sisse ehitatud infosüsteemide disaini, arhitektuuri ning äritegevusse, olles osa tuumfunktsionaalsusest. Andmetöötleja hindab korrapäraselt võimalikke ohte ning rakendab vastavalt olukorrale täiendavaid kaitsemeetmeid. Ta ei lükka omaenda hoolsuskohustusi kliendi õlgadele;

3) **andmetöötlus olgu algusest lõpuni turvaline**

Alates isikuandmete esmasest kogumisest kuni hävitamiseni on rakendatud asjakohased ja ajakohastatud turvameetmed. Nii on kindlustatud lõimitud andmekaitse rakendamine andmestiku kogu selle eluea ulatuses ehk „hällist hauani“;

4) **andmetöötlus olgu läbipaistev ja vastutustundlik**

Kõigile organisatsiooni andmetöötlusse kaasatud isikutele ning koostööpartneritele peab olema üheselt arusaadav, mis on andmetöötluse eesmärk. Andmesubjektile on tagatud teave nii tema andmete töötlemise eesmärgi kui ta õiguste kohta selle töötlemise suhtes. Avalikkusele/ andmesubjektile suunatud teave on kergelt kättesaadav ning selgelt ja lihtsalt sõnastatud. Vastutustundlik andmetöötlus tähendab ühtlasi, et organisatsioon on sõlminud

koostööpartneritega õiguspärased andmetöötluslepingud. Partneritele ei delegeerita vastutust, mis on organisatsiooni enda kohustus.

Nagu eelnevast loetelust näha, on tegu abistava spikriga isikuandmete kaitset tugevdava tehnoloogia ja töökorralduse juurutamiseks. Sõltuvalt andmete tundlikkusest ja ohtudest võib olla vajalik:

- kaheastmeline kasutaja tuvastamise lahendus, kus ei piisa üksnes salasõna teadmisest;
- isikuandmete edastamisel turvalahenduse kasutamine (nt TLS, VPN);
- kahe suhtluses osaleva poole sõnumiliikluse kaitse (nn *end-to-end protection*);
- logide varustamine digitaalse ajatempliga;
- isikuandmete pseudonüümimine või krüptimine;[21]
- isikuandmete anonüümimine, kui andmetöötluse põhieesmärk on saavutatud ning kogutud andmestikku kasutatakse lisaeesmärgina veel statistikaks või teadusuuringuiks.[22]

Näide: kui teenusega kaasneb identiteedi väärkasutamise oht – eriti suhtlus- ja tutvumisportaalides – siis tuleb teenusesse sisse ehitada kontrollmehhanism, mis välistab pahatahtlikult teise inimese kontaktandmete (nt e-post, telefoni nr) kasutamise. Selleks saab kasutada nt täiendava kinnituskoodi küsimist.

Mis on logid ja millal neid vaja on?

Andmetöötlustoimingutest tuvastatavate jälgede – logide – tekitamine ja nende haldamine on üks lõimitud andmekaitse rakendamise kesksemaid aspekte.

Otseselt on logipidamise kohustus kirjas õiguskaitseasutuste andmekaitsedirektiivis, mis on üle võetud IKS §-ga 36. Üldmääruse põhitekst ei maini isikuandmetega tehtavate toimingute logimist. Võib jääda ekslik mulje, et üldmääruse raames toimuvat isikuandmete töötlemist ei peagi logima?

Peab küll! Kõik organisatsioonid, kes oma tegevuse käigus isikuandmetega kokku puutuvad, on kohustatud tagama, et nende juures töödeldakse isikuandmeid turvaliselt. See tähendab muu hulgas, et infosüsteemides olevaid isikuandmeid kasutatakse ainult sel eesmärgil, mille jaoks nad kogutud on, ning keegi ei pääse andmetele ligi omakasupüüdlikel või pahatahtlikel eesmärkidel ega pelgast uudishimust. Selleks, et ära hoida isikuandmete väärkasutamist ning tagada, et tagantjärele oleks võimalik kindlaks teha, kes, millal ja miks infosüsteemis andmeid vaadanud või kasutanud on, peabki elektroonilise andmetöötluse puhul pidama logikirjeid isikuandmete töötlemise kohta.

Logipidamise alus tuleneb üldmääruse artiklite 5 ja 32 koosmõjust. Isikuandmete töötlemisel peab tagama andmete käideldavuse, [23] tervikluse [24] ning konfidentsiaalsuse. [25] Selleks peab

[21] **Pseudonüümine** tähendab äratuntavate isikuandmete asendamist varjunimede, numbrikoodide ja muude tunnustega, mida asjassepuutumatud isikud ei oska ära arvata. **Krüptimine** tähendab edastatava/hoitava teabe sisu kättesaamatuks muutmist. Lihtsaim viis krüptimiseks on ID-kaardiga krüptimine, krüptitud faile saavad avada vaid kindla isikukoodiga ID-kaardi valdajad.

[22] **Anonüümimine** tähendab teabest kõikide jälgede kaotamist, mis võiksid viia tuvastatavate isikuteni. Kui pseudonüümimine ja krüptimine on tagasipööratav umbisikustamine, siis anonüümimine tähendab tagasipööramatut ehk lõplikku umbisikustamist.

[23] Andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud isikule või tehnilisele vahendile.

[24] Andmete õigsuse, täielikkuse ja asjakohasuse tagatus ning veendumus, et andmed pärinevad autentsest allikast ning neid ei ole volitamata muudetud.

[25] Andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

andmetöötleja rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta andmeid loata või ebaseadusliku töötlemise eest.

Avalikus sektoris tuleneb logipidamise kohustus ka teistest õigusaktidest. Riigi- ja omavalitsusasutused, kes on teabevaldajad avaliku teabe seaduse tähenduses, ei saa juurdepääsupiiranguga teavet ilma logisid pidamata kaitsta.[26] Samuti peavad avaliku sektori asutused lähtuma valitsuse 20.12.2007 määrusest nr. 252 „Infosüsteemide turvameetmete süsteem" ning valitsuse 15.03.2012 määrusest nr. 26 „Infoturbe juhtimise süsteem", mille rakendamiseks on vajalik korrektne logipidamine.

Andmetöötlejal on ka kohustus tuvastada ning registreerida kõik isikuandmetega seotud rikkumised.[27] Need on oma sisult turvanõuete rikkumised, mis toovad kaasa töödeldavate isikuandmete juhusliku või ebaseadusliku kaotsimineku, hävimise, muutmise või loata juurdepääsu või avalikustamise.[28]

Seega logisid pidamata ei ole võimalik järgida isikuandmete töötlemise põhimõtteid ega tagada andmete töötlemise turvalisust.

Üldmäärus ei näe ette, millisel kujul logi peab pidama. Peaasi, et jälg jääks maha nii andmete sisestamise, muutmise, vaatamise, edastamise kui ka kustutamise kohta.

Logide tõendusväärtuse aitab tagada nende varustamine digitaalse ajatempliga. Lisaks tuleks läbi mõelda ja vastavalt organisatsiooni eripäradele paika panna logikirjete säilitamise tähtajad ning reeglid logide kontrollimiseks ja nendega tutvumiseks.

Mis on vaikimisi andmekaitse?

Vaikelahendus on see, mida kasutatakse algseadistusena, lähtevalikuna. Vaikelahendus peab olema kõige privaatsussõbralikum, kõige väiksemate ohtudega. Suuremaid ohte sisaldavad valikud peaksid olema need, mida inimene ise valib vaikelahenduse asemele.

Andmete kogumisel tuleb vältida, et üldkohustuslikud andmeväljad hõlmavad teavet, mida konkreetse inimese kohta vaja ei lähe. Vaikimisi tuleb nõuda vaid hädavajalikku minimaalteavet.

Näide A: *uues nutiseadmes ei ole traadita interneti ühendus (WiFi), Sinihammas (Bluetooth) ja asukohatuvastus vaikimisi sisse lülitatud. Kasutaja lülitab need ise sisse, kui selleks vajadus tekib;*
Näide B: *nutirakendus (äpp) ei küsi valimatult juurdepääsuõigusi kasutaja seadme funktsioonidele ja sisule. Lisamugavusi tagavate juurdepääsuõiguste mitteandmine ei ole takistuseks rakenduse põhifunktsioonide kasutamisel;*
Näide C: *võrgulehitseja (brauseri) turvaseaded ei võimalda vaikimisi inimese võrgukasutuse ulatuslikku jälgimist. Kasutaja ise võib algset kõrget turvataset allapoole tuua;*
Näide D: *kliendiks vormistamisel ei panna vaikimisi kohustuslikeks küsimusteks andmevälju, mida konkreetsele inimesele pakutavate teenuste puhul vaja ei lähe. Ei küsita vaikimisi igaühelt e-posti või telefoninumbrit – iga klient ei soovi saada ettevõttelt reklaami ega teateid. E-pood ei küsi mitteregistreerunud klientidelt, kes tellivad toote pakiautomaati, lisaks täpset elukoha aadressi – see on vajalik vaid juhul, kui on ette näha kullerteenuse kasutamist;*
Näide E: *kliendiks vormistamisel ei ole väljaspool lepingut kliendilt võetavad nõusolekud „ette ära linnutatud". Eeskätt käib see kliendi nõusoleku kohta saada ettevõttelt edaspidi reklaami;*
Näide F: *suhtluskeskkondades ja sotsiaal- ehk ühismeedias on andmete jagamine vaikimisi piiratud. Kasutaja ise otsustab, kellele ja millised andmeid ta kättesaadavaks teeb.*

[26] Vt avaliku teabe seadus § 43.
[27] Vt üldmäärus art 33.
[28] Vt isikuandmetega seotud rikkumise mõistet üldmäärus art 4.

Samas on selge, et kui inimene ise oma eraelu kaitsest ei hooli, siis ka teenuseosutaja ei saa teda vägisi kaitsta.

Lõimitud ja vaikimisi andmekaitse rakendamise õnnestumine sõltub suuresti eeltööst. Mida põhjalikumalt on andmetöötlus ning organisatsiooni tööprotsessid kaardistatud, infoturbe- ning andmekaitsealased riskid hinnatud ning maandatud, seda parem on lõpptulemus.

Eelkirjeldatud tegevused sisaldavad vältimatult organisatsiooni andmetöötluse ülevaate koostamist ning andmekaitseliste mõjude hindamist. Töötlusülevaadet käsitleme käesoleva üldjuhendi 4. peatükis, mõjuhinnangut selle sõna kitsamas tähenduses 5. peatükis.

3. peatükk. Andmekaitsespetsialist (AKS)

Vt. üldmääruse art. 37-39 ja pp. 97; direktiivi art. 32-34 ja pp. 63; IKS § 40-42;
Vt. Euroopa andmekaitseasutuste töörühma „Suunised andmekaitseametnike kohta".
Vt. inspektsiooni võrgulehel selgitused andmekaitsespetsialisti määramise kohta.

Kes peavad määrama andmekaitsespetsialisti?

Andmekaitseõigus muutub keerulisemaks, infotehniline areng toob kaasa üha uusi võimalusi ja ohte. Ettevõtted/asutused vajavad seetõttu üha enam andmekaitse alast oskusteavet. Mõnel juhul nõuab üldmäärus ja õiguskaitseasutuste andmekaitsedirektiiv (ning seda üle võttev IKS) andmetöötlejalt **andmekaitseametniku** määramist.

See ei ole õnnestunud eestikeelne terminivalik, sest ametnikud on üksnes avalikus teenistuses kas riigi või omavalitsuse ametiasutustes. Seetõttu kasutame kokkuleppeliselt **andmekaitsespetsialisti (AKS)** mõistet.[29]

Andmetöötlejatest peavad AKSi määrama:

1) kõik avaliku sektori asutused ja organid (v.a. kohtud õigusemõistmise osas);
2) need, kes jälgivad inimesi
   - oma põhitegevuse raames
   - korrapäraselt ja süsteemselt ning
   - sealjuures ulatuslikult;
3) need, kes töötlevad isikuandmete eriliike või süüteoandmeid ja süüdimõistavaid kohtuotsuseid
   - oma põhitegevuse raames ja
   - sealjuures ulatuslikult.

AKSi määramise kohustus on selline, mis võib kehtida nii vastutava kui volitatud andmetöötleja kohta.

> *Näide: väikesed poed tellivad klientide ostueelistuste väljaselgitamiseks ning isikustatud reklaami tegemiseks vajalikku andmeanalüütikat suurelt IT-ettevõttelt. Poodide endi püsiklientide arv on väike, neile teenust pakkuva IT-ettevõtte andmeanalüütika hõlmab aga kokku üle 50 tuhande inimese. Seega antud näites vastutavad töötlejad (poed) ise ei peagi AKSi määrama, küll aga peab seda tegema nende volitatud töötleja (IT-ettevõte).*

Kui ühe andmetöötluse raames määravad AKSi nii vastutav kui volitatud töötleja, siis peavad nad omavahel koostööd tegema.

Igasugune isikuandmete töötlemine ei tähenda alati jälgimist-monitoorimist.

> *Näide: pood peab küll püsiklientide üle arvestust raamatupidamisnõuete täitmiseks (arvete koostamiseks ja säilitamiseks), kuid klientide ostueelistuste analüüsi ei tee. Sel juhul ei ole kohustust AKSi määrata, sest kliente ei jälgita.*

Vaatame üle mõisted, millest oleneb AKSi määramise kohustus:

[29] Inglise keelde tõlgime selle termini ***data protection officer***, mitte ~~*data protection specialist*~~.

Kes on avaliku sektori asutus või organ?

AKSi peavad määrama kõik avaliku sektori asutused ja organid. Need on eeskätt riigi ja omavalitsuse asutused (näiteks põhiseaduslike institutsioonide kantseleid, valitsusasutused, valla- ja linnavalitsused; samuti eelloetletute poolt hallatavad asutused, näiteks koolid) ning avalik-õiguslikud juriidilised isikud (näiteks Eesti Rahvusringhääling, Kaitseliit, Rahvusraamatukogu, Eesti Pank, Eesti Haigekassa).

Teiseks paigutatakse avaliku sektori alla eraõiguslikud isikud, kui nad täidavad avalikku ülesannet. Eraõiguslikku avaliku ülesande täitjat aitab määratleda avaliku teabe seaduse § 5 lg 2: *„isik täidab seaduse, haldusakti või lepingu alusel avalikke ülesandeid, sealhulgas osutab haridus-, tervishoiu-, sotsiaal- või muid avalikke teenuseid*". Eraõiguslikule isikule, kes on avaliku ülesande täitmise tõttu avaliku teabe valdaja, laienevad ka isikuandmete kaitse alal avaliku sektori asutuse nõuded.

Näiteks tervishoiu alal loetakse avalikuks ülesandeks a) perearsti tegevust ambulatoorse üldarstiabi osutamisel, b) statsionaarse eriarstiabi osutamist piirkondlikus ja keskhaiglas ning c) kiirabi osutamist. [30] Samas ei välista avalik ülesanne võlaõiguslikku lepingulist suhet tervishoiuteenuse osutaja ja patsiendi vahel.

Riigi ja omavalitsuse asutatud eraõiguslik juriidiline isik (äri- või mittetulundusühing, sihtasutus) paigutatakse andmekaitse mõttes avalikku sektorisse, kui ta täidab avalikku ülesannet avaliku teabe seaduse § 5 lg 2 mõttes.

Mis on isikuandmete töötlemine põhitegevuse raames?

Põhitegevuse määratlemisel välistame sellest tugitegevused. Iseenda töötajate andmete töötlemine (nt. palga- ja puhkusearvestus, pääsuõiguste haldamine) ei ole põhitegevus.

Põhitegevus on see, milleks ettevõte/asutus on loodud, või mis on vähemalt üks tema võtmetegevusi. AKSi määramise kohustusega seonduv isikuandmete töötlemine peab olema sellise tegevuse lahutamatu osa. Näiteks ei ole ilma isikuandmete töötlemiseta võimalik osutada: a) tervishoiuteenust, b) finantsteenust, c) sideteenust, d) kindlustusteenust.

Mis on ulatuslik andmetöötlus?

Andmetöötluse ulatuslikkust saab määratleda väga erinevate näitajate põhjal. Euroopa andmekaitsenõukogu on soovitanud lähtuda näiteks:

- andmetöötluses hõlmatud isikute arvust või osakaalust asjaomases elanikkonnas;
- töödeldavate isikuandmete mahust ja/või erinevate andmekirjete arvust;
- isikuandmete töötlemise kestusest või pidevusest;
- isikuandmete töötlemise geograafilisest ulatusest.[31]

Inspektsioon eelistab suuremat selgust ning lähtub ulatuslikkuse määratlemisel eeskätt sellest, mitme inimese andmed on jälgimisse (nt. kliendiandmebaasis) hõlmatud:

[30] See kattub küberturvalisuse seaduse § 3 lg 1 punktides 6 ja 7 nimetatud oluliste tervishoiuteenustega.
[31] Vt Euroopa andmekaitsenõukogu „Suunised andmekaitseametnike kohta", p. 2.1.3 (25.05.2018 ülekinnitatud versioonis).

1) **eriliiki või süüteoandmed 5000 ja enama inimese kohta;**[32]

2) **suurt ohtu põhjustavad andmed 10 000 ja enama inimese kohta,**[33]
suure ohu näideteks võib tuua:

a.	identiteedivarguse või -pettuse oht (eriti digitaalse usaldusteenuse ning sellega võrreldava identiteedihaldusteenuse puhul)
b.	oht varale (eriti panga- ja krediitkaarditeenuse kaudu)
c.	oht sõnumisaladuse rikkumisele (eriti sideteenuse puhul)
d.	inimese asukoha reaalajas jälitamine (eriti sideteenuse puhul)
e.	inimese majandusliku seisu avalikuks saamine (eriti maksuandmete, pangaandmete ning krediidireitingu andmete kaudu – kuid see ei hõlma avalike andmete kasutamist)
f.	oht õiguslike tagajärgedega või samalaadse mõjuga diskrimineerimiseks (sealhulgas töövahendusteenuses ning palga- ja karjäärivõimalusi mõjutavas hindamisteenuses)

3) **ülejäänud isikuandmed 50 000 ja enama inimese kohta**.[34]

Mis on korrapärane ja süstemaatiline andmetöötlus?
1) mõiste ***korrapärane*** laieneb andmetöötlusele, mis toimub pidevalt või teatud ajavahemike tagant ega ei ole juhuslik;
2) ***süstemaatiline*** andmetöötlus on planeeritud ja metoodiline.[35]

Mis on jälgimine?

Üldmääruse pp. 24 viitab ***jälgimise*** osas näitena avalikus arvutivõrgus (internetis) toimuvale jälgimisele, eeskätt profiilianalüüsile, et teha inimese kohta otsuseid või analüüsida ja ennustada tema eelistusi, käitumist ja hoiakuid.

---

[32] Eriliiki isikuandmed on üldmääruse art. 9 ja direktiivi art. 10 nimetatud andmed. Süüteomenetluste andmeid ja süüdimõistvaid kohtuotsuseid käsitleb üldmääruse art. 10. Reeglina kehtivad nii eriliiki kui süüteoandmetele samasugused nõuded (vrd. üldmääruse art. 35 lg 3 p. b, art. 37 lg 1 p. c). Inspektsioon lähtus arvu 5000 osas üldmääruse pp. 91 toodud ulatuslikkuse selgitusest mõjuhinnangu tegemise kohustuse kontekstis. Pp. 91 kohaselt ei ole ulatuslik töötlemine üksiku arsti või muu tervishoiutöötaja andmetöötlus. Üldmäärus ei ütle, mitmest tervishoiutöötajast algab ulatuslik töötlemine. Eestis on kõige levinuimaks üksikuks tervishoiutöötajaks perearst, kelle nimistu piirsuurus on tervishoiuteenuste korraldamise seaduse § 8 lg 4^1 kohaselt 2000 patsienti või koos abiarstiga tegutsedes 2400 (tegelikkuses tavaliselt suurem). Arv 5000 tähendab vähemalt 3 piirarvu sisse jäävat perearsti või 2 piirarvust suuremat perearsti. Selle näite puhul tuleb arvestada, et ulatuslikkus on perearsti puhul oluline mõjuhinnangu tegemise kohustuse, mitte AKSi määramise kohustuse osas (kuna perearst kuulub avalikku sektorisse). Üldmääruse põhjenduspunktis toodud näide viitab ka üksikult tegutsevale juristile, kuid juristide klientuuri kohta usaldusväärne arvuline teave puudub. Ühtlasi arvestame, et eriliiki isikuandmete kohta käivad üldmääruse normid on rangemad kui varasemalt kehtinud isikuandmete kaitse seaduses – nende töötlemise alused on sõnastatud erandina, reegliks on keeld (vrd art. 9 lg 1, samuti direktiivi art. 10 lg 1; vt ka IKS § 20). Seetõttu on mõistlik, et eriliiki isikuandmete puhul kehtib muudest tundlikumatest andmetest poole väiksem ulatuslikkuse näitaja.
[33] Suure ohu määratlus – vt üldmääruse pp. 75. Arvu 10 000 puhul lähtub inspektsioon võrreldavusest teiste oluliste teenustega, kus kasutatakse samuti 10 000 kliendi kriteeriumit: nt. oluline kaabelleviteenus (küberturvalisuse seaduse § 3 lg 1 p 5), elutähtsa teenusena osutatava elektrijaotusvõrgu teenus (elektrituruseaduse § 21^1 p. 4), elutähtsa teenusena osutatav gaasijaotusvõrgu teenus (maagaasiseaduse § 22 lg 15 p. 2).
[34] Ülejäänud andmete töötlemise ulatuslikkuse puhul lähtus inspektsioon üldmääruse pp. 75 viimasest lauseosast: „***kui töötlemine hõlmab suurt hulka isikuandmeid ja mõjutab paljusid andmesubjekte***".
[35] Vt. põhjalikumalt lisast 4.

Jälgimise mõiste ei piirdu siiski ainult veebikeskkonnaga, internetis jälgimine on vaid üks võimalusi. Jälgimine toimub näiteks püsiklientide ehk tuvastatud klientide kohta nende ostuajaloo analüüsimise kaudu. Inimese kohta eri allikatest sarnaste andmete kokku kogumine on samuti jälgimine (näiteks krediidivõimelisuse hindamiseks, ühendades inimese kohta saadavaolevad avalikud andmed võlausaldajatelt saadud mitteavalike andmetega). Jälgimine on ka inimese asukoha-andmete jälgimine tema teenuste või seadmete kaudu.

Kaamera võimaldab vaateväljas olevat inimest äratundavalt jälgida (sh suumida). Eriti tõhus jälgimine toimub näotuvastus-tarkvara kasutades. Ühekordne droonikaamera lennutamine ning suures plaanis avalike alade (nt väljakute) mittesuumitav kaamerapilt ei lähe inimeste jälgimise alla.

Kes saab olla AKSiks?

AKSi rolli võib täita:

- andmetöötleja oma töötaja (täistöökoht või lisaülesanne) või
- andmetöötleja väline füüsiline või juriidiline isik (nt teenuslepingu alusel).

Isegi kui tegelikult kasutatakse „kollektiivse AKSi" mudelit (s.t. AKSi ülesanded on pandud mõnele omaenda osakonnale vms allüksusele), peab välispidiselt (avalikkuse ja inspektsiooniga suhtlemiseks) keegi olema nimeliselt AKSiks määratud.

Avalikus sektoris on üldmääruse rakendusettevalmistuse käigus määratud suuremates asutustes täiskohaga AKS-id, väiksemates antud lisaülesandena. Nii ühel kui teisel juhul on neile tagatud tugi (paika pandud koostöösuhted infoturbe-, asjaajamis-, avalike suhete, õigusala jt vajalike kolleegidega).

AKSile – sarnaselt raamatupidajaga – ei ole kehtestatud diplomi- ega muid formaalseid kvalifikatsiooninõudeid. Soovitav on siiski, et tal oleks asjakohane koolitus täiend- või diplomiõppena läbitud.

Inspektsioon loodab, et tulevikus suudetakse AKSi kvalifikatsiooniküsimused lahendada kutseseaduse alusel kutsestandardiga.

AKS peab olema võimeline suhtlema nii andmesubjektide kui inspektsiooniga eesti keeles.

Mis on AKSi ülesanded?

AKSi ülesanded:

- olla andmesubjektidele kontaktisikuks kõigis küsimustes, mis on seotud nende isikuandmete töötlemise ja nende andmekaitseliste õiguste kasutamisega;
- teavitada ja nõustada oma organisatsiooni (vajadusel ka selle partnerite) juhtkonda ning personali andmekaitse alal;
- jälgida andmekaitsenormide rakendamist, sealhulgas vastutusvaldkondade jaotamist, personali teadlikkust ja koolitamist, ning andmekaitselist auditeerimist;
- anda nõu seoses andmekaitsealase mõjuhinnanguga ning jälgida selle toimimist;
- teha koostööd Andmekaitse Inspektsiooniga, olles tööandja kontaktisikuks.

Need on üldmäärusest/direktiivist (ehk sisuliselt IKS-st) tulenevad AKSi põhiülesanded. Iseenesest ei sega see andmast talle ka muid tööülesandeid – kui see ei takista põhiülesannete täitmist.

Paratamatult täidab AKS „tõlgi“ rolli – ta peab oskama andmekaitset selgitama nendele, kes ei ole selle ala spetsialistid. See nõuab erialažargoonist, eriti aga võõrkeelsetest sõnadest/lühenditest hoidumist.

Avalikus sektoris peab inspektsioon hädavajalikuks panna asutuse AKSile ka avaliku teabe seaduse rakendamise osas analoogsed ülesanded. Isikuandmete kaitse, avaliku teabe kättesaadavus ja avaliku teabe juurdepääsupiirangud on asutuse töös läbi põimunud. Seetõttu neil peaks olema ka sama koordinaator.

AKS peab oskama siduda õiguslikke ja tehnilisi teadmisi oma ettevõtte/asutuse tegeliku tööga, „köögipoolega“. See võib muuta väljast sisse ostetud teenusepakkuja kasutamise kasuteguri küsitavaks.

Inspektsioon on täiendavalt koostanud nimekirja soovituslikest kompetentsidest, mis on eelduseks AKSi rolli tulemuslikuks täitmiseks.

Kuidas AKSi määramisest teada anda?

Kui AKS on määratud, tuleb sellest teada anda nii avalikkusele kui Andmekaitse Inspektsioonile. Mõlemat ühekorraga saab tööandja teha äriregistri ettevõtjaportaali kaudu – sinna sisestatud AKSi näeb nii avalikkus kui inspektsioon. Inspektsioonile ei ole enam eraldi teadet vaja saata. Täpsemad juhised on inspektsiooni võrgulehel.

Arusaadavalt saab andmetöötleja nimel teadet esitada vaid allkirjaõiguslik esindaja või tema volitatud isik, kes esitab ka volikirja. Üks ettevõte/asutus ei saa esitada ilma volituseta teise ettevõtte/asutuse AKSi – isegi kui ta on sama kontserni ettevõte või kõrgemalseisev asutus.

Kindlasti andke AKSi määramisest teada ka oma töötajatele. Ettevõtte/asutuse töökorraldus peaks tagama, et töötajad teaksid andmekaitselistes küsimustes kõigepealt omaenda AKSi poole pöörduda. Ilma selleta läheb info temast mööda.

Kui ettevõttes/asutuses, kus AKS on määratud, hakatakse inspektsiooni poole temast mööda minnes pöörduma, on see inspektsioonile kindel märk, et AKSi määramine sellises ettevõttes/asutuses on vaid paberi peal tehtud formaalsus ja tegelikult on asjad halvad.

Mis saab delikaatsete isikuandmete töötlemise eest vastutavatest isikutest?

Varasem seadus nõudis delikaatsete isikuandmete töötlejatelt kas töötlemise registreerimist inspektsioonis või alternatiivina töötlemise eest vastutava isiku määramist. Ka sellest määramisest tuli inspektsioonile teada anda.

Kuna nõuded on erinevad, siis senistest vastutavatest isikutest automaatselt AKSe ei saa. Alates 2018. a. 25. maist on delikaatsete isikuandmete töötlemise register suletud ning arhiveeritakse.

4. peatükk. Isikuandmete töötlemisülevaade

Vt. üldmääruse art. 30 ja pp. 39; direktiivi art. 24 ja pp. 56; IKS § 37
Vt. näidised inspektsiooni võrgulehel

Miks seda vaja on ja kes selle koostama peavad?

Üldmääruse ja direktiivi üks läbivaid põhimõtteid on andmetöötleja vastutus. Andmetöötleja vastutab inimeste suhtes seadusliku, õiglase ning läbipaistva andmetöötluse korraldamise eest.[36]

Seda kõike ei saa teha, kui andmetöötlejal ei ole omaenda andmetöötlusest täit pilti. Seetõttu peab ta kaardistama oma andmetöötlustoimingud. Nimetame selle tulemusena valminud dokumenti **isikuandmete töötlemisülevaateks**.

Ülevaade on see, mida peavad silmas üldmääruse art. 30 ja direktiivi art. 24 (seda üle võttev IKS § 37). Kumbki neist artiklitest ei pea silmas iga üksiku toimingu tegemist sisaldavat registrit-logiraamatut (vaatamata üldmääruse ja direktiivi artikli ebaõnnestunud pealkirjale).

Üldmääruse art. 30 on ebaõnnestunud sõnastusega ka ses osas, kellele see kohustus on suunatud. Art. 30 lg 5 loob esmalt väära mulje, nagu kehtiks see vaid andmetöötlejatele, kellel on 250 ja enam töötajat. Tegelikult ütleb see säte muuhulgas, et ülevaate peavad koostama kõik, kelle andmetöötlus ei ole juhuslik. Kui aga ettevõttel/asutusel on vähemalt üks töötaja ja/või vähemalt üks füüsilisest isikust klient, siis nende andmete töötlemine ei ole juhuslik.

Lõige 5 sisaldab veel kahte erisust ülevaate koostamise nõude osas – seda tuleb teha ka a) eriliiki ning süüteoandmete töötlemise korral, b) samuti siis, kui andmetöötlus kujutab endast tõenäolist ohtu. Mittejuhusliku andmetöötluse erisus on aga niivõrd lai, et neil kahel lisaerisusel puudub praktiline tähendus.

Kokkuvõtlikult: üldmäärus kohustab kõiki andmetöötlejaid, kellel on vähemalt üks töötaja ja/või vähemalt üks füüsilisest isikust klient, koostama isikuandmete töötlemise ülevaate.

Direktiiv ning IKS on ses osas õnneks selge, pannes ülevaate koostamise nõude kõigile õiguskaitseasutustele.

Millega tasub töötlemisülevaate koostamist ühitada?

Inspektsioon soovitab ülevaate koostamise ühitada teiste dokumentide koostamisega, mis samuti käsitlevad andmehaldust ettevõttes/asutuses. Säästate omaenda aega ja energiat, kui ühitate kaardistamise/dokumenteerimise. Lisaks on tulemus kvaliteetsem, sest väldite dokumentide vahel vastuolusid.

Soovitus ettevõtetele – samaaegselt töötlusülevaate koostamisega koostage/uuendage järgmisi dokumente:

a) avalikud andmekaitsetingimused (vt selle juhendi 10. ptk, üldmääruse art. 12 jj),
b) kui olete elutähtsa/olulise teenuse osutaja küberturvalisuse seaduse mõttes (§ 7 lg 2 p. 1-2), siis riskianalüüs,

[36] Vt üldmääruse art. 5 lg 1 p. a ja lg 2; direktiivi art. 4 lg 1 p. a ja lg 4.

c) kui kavandate mingit uut tundlikku ulatuslikku andmetöötlust, siis andmekaitseline mõjuhinnang (vt selle juhendi 5. ptk, üldmääruse art. 35).

Soovitus asutustele – samaaegselt töötlusülevaate koostamisega koostage/uuendage järgmisi dokumente:

a) avalikud andmekaitsetingimused (vt selle juhendi 10. ptk, üldmääruse art. 12 jj, direktiivi art. 12 jj, IKS § 22 jj, lisaks avaliku teabe seaduse § 28 lg 1 p. 31^1),
b) riskianalüüs küberturvalisuse seaduse kohaselt (§ 7 lg 2 p. 1-2),
c) kui kavandate mingit uut tundlikku ulatuslikku andmetöötlust, siis andmekaitseline mõjuhinnang (vt selle juhendi 5. ptk, üldmääruse art. 35, direktiivi art. 27, IKS § 38).
d) isikuandmeid sisaldava teabe avaandmeteks tegemisel mõjuhinnang (avaliku teabe seaduse § 3^1 lg 3);
e) teenuste ülevaade (valitsuse määruse „Teenuste korraldamise ja teabehalduse alused" § 12);
f) dokumentide liigitusskeem (valitsuse määruse „Arhiivieeskiri" §-d 6-8).

Mida peab töötlemisülevaade sisaldama?

Vastutava töötleja ülevaade peab sisaldama vähemalt järgmist:

- vastutava töötleja, kaasvastutava töötleja (kui on), vastutavate töötlejate (kui on) ja andmekaitsespetsialisti (kui on) nimi ja kontaktandmed;
- isikuandmete töötlemise eesmärgid;
- andmesubjektide kategooriate ja isikuandmete liikide kirjeldus;
- vastuvõtjate kategooriad, kellele isikuandmed avalikustatakse;
- kui isikuandmeid edastatakse kolmandasse riiki, siis andmed selle kohta koos riigi nimega, ning muu teave edastamise asjaolude ja kaitsemeetmete kohta;[37]
- eri andmeliikide kustutamiseks ette nähtud tähtajad;
- turvameetmete üldine kirjeldus.

Lisaks vastutavale töötlejale peab ülevaate koostama ka volitatud töötleja. Näiteks raamatupidamis- ja personaliarvestusteenuseid osutav ettevõte on oma lepingupartnerite volitatud töötleja. Volitatud töötleja andmetöötlusülevaade peab sisaldama vähemalt:

- volitatud töötleja enda, vastutava(te) töötleja(te), teiste volitatud töötlejate (kui on) ning omaenda andmekaitsespetsialisti (kui on) nime ja kontaktandmeid;
- vastutava töötleja nimel tehtava töötlemise kategooriaid (seda on kõige lihtsam esitada viitega teenuse nimetusele, nt. andmemajutus-, raamatupidamis-, logistika-, inkassoteenus – vajadusel täpsustage, kellele mis teenuseid osutate);
- kui isikuandmeid edastatakse kolmandasse riiki, siis teave selle kohta koos riigi nimega, ning muu teave edastamise asjaolude ja kaitsemeetmete kohta;[38]
- turvameetmete üldist kirjeldust.

[37] Silmas peetakse riike ja rahvusvahelisi organisatsioone väljaspool Euroopa majanduspiirkonda. Euroopa majanduspiirkond on Euroopa Liit ning Island, Norra ja Liechtenstein.
[38] Silmas peetakse riike ja rahvusvahelisi organisatsioone väljaspool Euroopa majanduspiirkonda. Euroopa majanduspiirkond on Euroopa Liit ning Island, Norra ja Liechtenstein.

Arusaadavalt vajab ülevaade aja- ja asjakohastamist, kui andmetöötluses toimuvad olulised muutused.

Avaliku sektori asutuste osas peab inspektsioon vajalikuks veeru lisamist avaliku teabe režiimi kohta. Näidake andmeliikide kaupa, milline on nende juurdepääsetavus: kas a) juurdepääsupiiranguga teave, b) teabenõudega küsitav teave , c) võrgulehel avaldatav teave, d) avaandmed.[39]

Ülevaate mõnest veerust lähemalt

Eesmärk:
Isikuandmete töötleja peab suutma põhjendada seost kogutavate andmete ning nende töötlemise eesmärgi vahel. Kindlasti ei saa eesmärgiks olla andmete kogumine/töötlemine iseenesest, see on vahend eesmärgi saavutamiseks.

Eesmärgina ei saa näidata ka töötlemise alust (näiteks „avaliku võimu teostamine“ või „lepingu täitmine“). Eraõigusliku isiku puhul on tavaliselt eesmärgiks teenuse osutamine (nt veoteenus, raamatupidamisteenus, elukindlustusteenus, andmesideteenus jne).

Andmesubjektide kategooriad
Teenuseosutajate puhul on ettevõtte-välisteks andmesubjektideks eeskätt nende kliendid. Samuti töödeldakse füüsilisest isikust koostööpartnerite andmeid, võib-olla ka juriidilisest isikust koostööpartnerite töötajate andmeid. Maja-sisese andmetöötluse subjektideks on omaenda töötajad ja praktikandid. Kui majas käib palju külastajaid, kelle isikud tuvastatakse, siis ka nemad.

Andmesubjektide kategooriaid võib vastavalt vajadusele moodustada ka teistel alustel. Näiteks õpilased, lapsevanemad, üliõpilased, õpetajad/õppejõud, tugipersonal jne.

Isikuandmete liigid
Töötlusülevaate koostamise puhul tuleb kasutada mõistliku detailsusastmega liigitust. Toome näiteks võimaliku kliendiandmete liigutuse: nimi, kasutajatunnus, sidevahendite andmed, ostuajalugu, ette- ja järelmaksuandmed, võlgnevusandmed, ostueelistuste analüüs, kliendisuhte tekkimise ja lõppemise aeg, nõusolek saada reklaami.

Millises vormis peab töötlusülevaade olema?

Üldmääruse nõuab, et ülevaade peab olema kirjalikus või elektroonilises vormis, suulisest ei piisa. Muid vormistusnõudeid ei ole.

Ülevaade võib olla nii ühes kui mitmes dokumendis. Näiteks asutus võib lugeda oma ülevaate osaks enda peetava andmekogu kirjelduse riigi infosüsteemi haldussüsteemis, kui see sisaldab üldmääruse artiklis 30 nõutud teavet.

Andmekaitse Inspektsioon võib andmetöötlejalt ülevaate välja nõuda, seega tuleb tagada, et ülevaate elektrooniline vorming võimaldaks kopeerimist ja avamist.

[39] Kõik avalikud andmed avaliku teabe seaduse järgi ei ole automaatselt avaandmed. Avaandmed on digitaalandmed, mille teabevaldaja on andmekogumina teinud masinloetaval kujul avatud vormingus kättesaadavaks ja sellisena tähistanud. Erinevalt muudest avalikest andmetest ei kehti isikuandmeid sisaldavatele avaandmetele mingid edasikasutamise piirangud. Seetõttu tuleb enne andmete avaandmeteks andmist viia läbi avaliku teabe seaduse §-s 3^1 ettenähtud mõju hindamine.

5. peatükk. Andmekaitsealane mõjuhinnang

Vt üldmääruse art. 35, pp. 89-93; direktiivi art. 27, pp. 51-53; IKS § 38.
Vt käesoleva üldjuhendi lisa nr. 1 „Andmekaitsealase mõjuhinnangu tegemise kontrollnimekiri".
Vt. Euroopa andmekaitsenõukogu „Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht" vastavalt määrusele (EL) 2016/679".
Vrd. küberturvalisuse seaduse riskianalüüsi sätetega, eeskätt § 7.

Miks on mõjuhinnangut vaja? Mida ta sisaldab?

Iga mõistlik andmetöötleja hindab nii või teisiti oma tänaseid ja tulevasi ohte, kui selleks on vajadus. Õiguslikus mõttes on seda vaja kolme nõude täitmiseks:
1) vastutaval töötlejal on kohustus võtta arvesse andmetöötlusega seotud ohte ning rakendada meetmeid, et tagada andmetöötluse vastavus üldmäärusele/direktiivile ning seda üle võtvale IKS-le ja olla võimeline seda vastavust tõendama;[40]
2) vastutaval töötlejal on kohustus rakendada lõimitud andmekaitset;[41]
3) vastutaval ja volitatud töötlejal on kohustus tagada töötlemise turvalisus.[42]

Ulatusliku tundliku isikuandmete töötlusega alustamisel nõuab üldmäärus/direktiiv (IKS) mõju hindamist dokumenteeritud kujul. Selle dokumendi sisule seatakse mõned miinimumnõuded. Vastutav töötleja hindab ja kirjeldab:

1)	mis eesmärgi saavutamiseks mis alusel mis isikuandmeid mis meetoditega ta töötleb
2)	kuidas töötlemiseks kavandatud valikud on eesmärgi saavutamiseks vajalikud ja kohased
3)	ohtude analüüs, sh nende taseme määramine (nt kõrge, keskmine, madal)
4)	milliseid tagatisi ja meetmeid ta ohtude suhtes rakendab

See ongi mõjuhinnangu sisu miinimum. Meetmed kätkevad endast töökorralduse reegleid, füüsilisi ja infotehnilisi lahendusi.

Mõjuhinnangu kõige olulisem eesmärk on hinnata, kas andmete kaitseks rakendatavad meetmed on piisavad, et tõenäolisi ohte kas täielikult maandada või vähemalt leevendada vastuvõetavale tasemele.

Kes peavad mõjuhinnangu tegema?

Mõjuhinnangu peavad tegema kõik isikuandmete vastutavad töötlejad, kelle isikuandmete töötlemise **laadi**, **ulatust**, **konteksti** ja **eesmärke** arvestades tekib tõenäoliselt inimestele **suur oht**.[43]

Üldmääruse eestikeelne versioon (art. 35 lg 3) toob eelneva kohta kolm näidet.[44] Esimene näide käib profileerimise kohta: andmetöötleja hindab inimesi

a. automatiseeritud andmetöötlust kasutades

[40] Vt üldmääruse art. 24, direktiivi art. 19, IKS § 29 lg 1.
[41] Vt üldmääruse art. 25 lg 1, direktiivi art. 20 lg 1, IKS § 33.
[42] Vt üldmääruse art. 32, direktiivi art. 29, IKS § 43.
[43] Andmetöötluse laadi, konteksti ja eesmärki selgitame lisas nr 4. Andmetöötluse ulatust selgitame käesolevas peatükis.
[44] Direktiivi art. 27 näidiste loetelu ei sisalda.

b. ulatuslikult ja
c. süstemaatiliselt ning
d. selline hindamine on inimesele kas õiguslike tagajärgedega või olulise mõjuga.

Teine näide seisneb eriliiki või süüteoandmete ulatuslikus töötlemises.

Kolmas näide on avalike alade ulatuslik süstemaatiline jälgimine.

Paraku on üldmääruse eestikeelsest tõlkest jäänud ekslikult välja asjaolu, et see loetelu on tegelikult lahtine. Need näited ei ole ammendavad. Seega vajab mõjuhinnangut ka muu andmetöötlus, millega võib tõenäoliselt kaasneda eelneva kolme näitega võrreldav suur oht.

Mõjuhinnangu tegemise kohustuse määratlemisel tulevad mängu kaks kriteeriumi, mida üldmäärus kasutab ka andmekaitsespetsialisti määramise kohustuse juures: a) töötlemise ***süstemaatilisus*** ja b) ***ulatuslikkus***.[45] Kordame nende definitsioone:

Süstemaatiline andmetöötlus on planeeritud ja metoodiline. Andmetöötlus on ***ulatuslik***, kui hõlmab:

1) **eriliiki või süüteoandmeid 5000 ja enama inimese kohta;**[46]

2) **suurt ohtu põhjustavaid andmeid 10 000 ja enama inimese kohta;**[47]
suure ohu näideteks võib tuua:

a. identiteedivarguse või -pettuse oht (eriti digitaalse usaldusteenuse ning sellega võrreldava identiteedihaldusteenuse puhul)
b. oht varale (eriti panga- ja krediitkaarditeenuse kaudu)
c. oht sõnumisaladuse rikkumisele (eriti sideteenuse puhul)
d. inimese asukoha reaalajas jälitamine (eriti sideteenuse puhul)
e. inimese majandusliku seisu avalikuks saamine (eriti maksuandmete, pangaandmete ning krediidireitingu andmete kaudu – kuid ei hõlma avalike andmete kasutamist)
f. oht õiguslike tagajärgedega või samalaadse mõjuga diskrimineerimiseks (sealhulgas töövahendusteenuses ning palga- ja karjäärivõimalusi mõjutavas hindamisteenuses)

[45] Vt üldmääruse art. 37 lg 1 p. b ning ulatuslikkuse osas ka p. c. Andmekaitsespetsialistidest lähemalt käesoleva üldjuhendi ptk. 3.

[46] Eriliiki isikuandmed on üldmääruse art. 9 ja direktiivi art. 10 nimetatud andmed. Süüteomenetluste andmeid ja süüdimõistvaid kohtuotsuseid käsitleb üldmääruse art. 10. Reeglina kehtivad nii eriliiki kui süüteoandmetele samasugused nõuded (vrd. üldmääruse art. 35 lg 3 p. b, art. 37 lg 1 p. c). Inspektsioon lähtus arvu 5000 osas üldmääruse pp. 91 toodud ulatuslikkuse selgitusest. Pp. 91 kohaselt ei ole ulatuslik töötlemine üksiku arsti või muu tervishoiutöötaja andmetöötlus. Üldmäärus ei ütle, mitmest tervishoiutöötajast algab ulatuslik töötlemine. Eestis on kõige levinuimaks üksikuks tervishoiutöötajaks perearst, kelle nimistu piirsuurus on tervishoiuteenuste korraldamise seaduse § 8 lg 4^1 kohaselt 2000 patsienti või koos abiarstiga tegutsedes 2400 (tegelikkuses tavaliselt suurem). Arv 5000 tähendab vähemalt 3 piirarvu sisse jäävat perearsti või 2 piirarvust suuremat perearsti. Selle näite puhul tuleb arvestada, et ulatuslikkus on perearsti puhul oluline mõjuhinnangu tegemise kohustuse, mitte AKSi määramise kohustuse osas (kuna perearst kuulub avalikku sektorisse). Üldmääruse põhjenduspunktis toodud näide viitab ka üksikult tegutsevale juristile, kuid juristide klientuuri kohta usaldusväärne arvuline teave puudub. Ühtlasi arvestame, et eriliiki isikuandmete kohta käivad üldmääruse normid on rangemad kui varasemalt kehtinud isikuandmete kaitse seaduses – nende töötlemise alused on sõnastatud erandina, reegliks on keeld (vrd art. 9 lg 1, samuti direktiivi art. 10 lg 1; vt ka IKS § 20). Seetõttu on mõistlik, et eriliiki isikuandmete puhul kehtib muudest tundlikumatest andmetest poole väiksem ulatuslikkuse näitaja.

[47] Suure ohu määratlus – vt üldmääruse pp. 75. Arvu 10 000 puhul lähtub inspektsioon võrreldavusest teiste oluliste teenustega, kus kasutatakse samuti 10 000 kliendi kriteeriumit: nt. oluline kaabelleviteenus (küberturvalisuse seaduse § 3 lg 1 p 5), elutähtsa teenusena osutatava elektrijaotusvõrgu teenus (elektrituruseaduse § 21^1 p. 4), elutähtsa teenusena osutatav gaasijaotusvõrgu teenus (maagaasiseaduse § 22 lg 15 p. 2).

g.	laste isikuandmete töötlemine (lastele suunatud teenustes)
h.	seadusest tuleneva saladuse hoidmise kohustusega kaitstud teabe avalikuks saamise oht (juurdepääsupiiranguga teave, ameti- ja kutsesaladusega kaitstud teave)

3) **ülejäänud isikuandmed 50 000 ja enama inimese kohta**.[48]

Piiriülese andmetöötluse korral[49] ei määratletata ulatuslikku töötlemist andmesubjektide täpse minimaalse arvu järgi. Seetõttu peavad vastutavad töötlejad piiriüleste isikuandmete töötlemisel järgima järgmisi nõudeid.

Järgnev loetelu on soovituslik ning esitatud näited täiendavad ja täpsustavad täiendavalt üldmääruse artikli 35 lõikes 1 sätestatud nõudeid ning kriteeriume, mis on loetletud juhendis „*Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht" vastavalt määrusele (EL) 2016/679*".

Iga vastutav töötleja peab läbi viima andmekaitsealase mõju hindamise, kui võttes arvesse töötlemise laadi, ulatust, konteksti ja eesmärke, on tõenäoline, et füüsilisele isikule tekib suur oht.

Üldmääruse artikli 35 lõige 3 annab selle kohta kolm näidet.

1. Esimene näide on profileerimine - vastutav töötleja / volitatud töötleja hindab inimesi:

   a. automatiseeritud andmetöötlemist kasutades
   b. ulatuslikult (suures ulatuses)
   c. süstemaatiliselt ning
   d. selline hindamine on inimesele õiguslike tagajärgedega või olulise mõjuga.

2. Teine näide on eriliigiliste andmete või kriminaalkorras süüdimõistvate kohtuotsuste andmete ulatuslik töötlemine.

3. Kolmas näide on avalike alade ulatuslik süstemaatiline jälgimine.

Euroopa Andmekaitsenõukogu suunistest [50] lähtudes tuleks kaaluda järgmisi tegureid, kui otsustatakse, kas töötlemine toimub suures ulatuses:

   a. asjaomaste andmesubjektide arv kas konkreetse numbri või asjaomase elanikkonna osana;
   b. andmete maht ja/või töödeldavate erinevate andmeühikute hulk;
   c. andmete töötlemise kestus või püsivus;
   d. töötlemistoimingute geograafiline ulatus.

Üldmääruse artikli 35 lõikes 3 loetletud näited ei ole ammendavad. Seetõttu vajab andmekaitse mõju hindamist ka muud liiki isikuandmete töötlemine, mis võib kaasa tuua eelneva kolme näidisega võrreldava kõrge riski. Näiteks:

4. Biomeetriliste andmete ulatuslik töötlemine füüsilise isiku ainulaadse identifitseerimise eesmärgil.

5. Geneetiliste andmete töötlemine suures ulatuses.

---

[48] Ülejäänud andmete töötlemise ulatuslikkuse puhul lähtus inspektsioon üldmääruse pp. 75 viimasest lauseosast: ***„kui töötlemine hõlmab suurt hulka isikuandmeid ja mõjutab paljusid andmesubjekte***".

[49] Üldmääruse artikkel 35 lõige 6

[50] Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht" vastavalt määrusele (EL) 2016/679 ja Suunised andmekaitseametnike kohta

6. Tööhõive kontekstis ulatuslik andmete töötlemine hõlmates töötajate tegevuste süstemaatilist jälgimist.

Ulatuslik töötlemine, mis:

7. Võib kujutada endast identiteedivarguse või pettuse ohtu (eriti digitaalsete usaldusteenuste ja võrreldavate identiteedi haldamise teenuste puhul).

8. Võib tekitada varalise kahju riski (eriti pangandus- ja krediitkaarditeenuste puhul).

9. Võib põhjustada kirjavahetuse saladuse rikkumise ohtu (eriti sideteenuste puhul).

10. Toob kaasa asukoha jälgimise reaalajas (eriti sideteenuste puhul).

11. Võib kujutada ohtu isiku majandusliku seisu avalikustamisele (eriti maksualased andmed, pangandusandmed, krediidireitingu andmed - avalikult kättesaadavaid andmeid ei võeta arvesse).

12. Võib kujutada diskrimineerimise ohtu, millel on õiguslikud tagajärjed või millel on sarnane mõju (eriti tööjõu vahendamise ning palka ja karjääri mõjutavate hindamisteenuste puhul).

13. Võib kujutada ohtu, et kaotatakse teabe seadusjärgne konfidentsiaalsus (piiratud teave, ametisaladus).

Rõhutame, et eelnevalt mainitud nimekirjad ja näited ei ole ammendavad, kuna näited üldmääruse artikli 35 lõikes 3 ei ole ammendavad.

Kuidas mõjuhinnangut koostada?

1) mõjuhinnangu peab koostama elektroonilises/kirjalikus vormis. Ta on küll andmetöötleja sisemine dokument, kuid Andmekaitse Inspektsioon võib selle järelevalve käigus välja nõuda ning eelkonsulteerimise käigus on selle inspektsioonile esitamine nõutav;

2) juhul, kui andmetöötlejal on küberturvalisuse seaduse kohaselt nõutav riskianalüüsi koostamine, siis on mõistlik küberturbe-ohtude hindamine ühitada isikuandmete kaitse alase mõju hindamisega;

3) andmekaitsealane mõju hindamine ei ole ühekordne tegevus. Kui andmetöötluse käigus ilmnevad uued suured ohud (näiteks kasutatav tark- või riistvara muutub infotehnilise arengu tõttu haavatavaks ning terve infosüsteemi turvalisus satub ohtu), siis tuleks mõjuhinnangut uuendada. Arusaadavalt kehtib siin olulisuse printsiip – ebaoluliste muutuste pärast ei ole mõtet mõjuhinnangut uuendama hakata;

4) sarnast suurt ohtu kujutavaid andmetöötlusi võib hinnata koos. Koos hindamist võiks teha ka siis, kui andmetöötlusse on kaasatud mitu andmetöötlejat (kaasvastutavad töötlejad ja/või vastutav ja volitatud töötleja). Eriti oluline on sel juhul täpselt fikseerida vastutus kaitsemeetmete osas;

Näide A: kaupluste ja turvaettevõtte koostöö kaameravalve kasutamise mõjuhinnangu tegemisel
Näide B: asutuste koostöö sama dokumendihaldusplatvormi kasutusele võtu mõjuhinnangu tegemisel

5) mõjuhinnangu tegemisse tuleb kaasata andmekaitsespetsialist, kui ta on või peab olema ettevõttes/asutuses määratud;[51]

6) kui on nõutav mõjuhinnang tegevusele, mis põhineb õigusaktil (avaliku võimu teostamine, avaliku ülesande täitmine, seadusejärgne kohustus), siis võib olla mõistlik teha mõjuhinnang ära

[51] Andmekaitsespetsialistist lähemalt vt käesoleva üldjuhendi 3. peatükist.

juba õigusakti eelnõu väljatöötamiskavatsuse juures ja lisada ka peatükina eelnõu seletuskirja. Kui kõik olulised asjaolud olid juba väljatöötamiskavatsuse ajal teada ja nad hinnati ära, siis õigusakti rakendavad asutused täiendavat mõjuhinnangut koostama ei pea. Kui aga olulisi andmetöötlusvalikuid, mis põhjustavad suurt ohtu, tehakse alles või lisaks ka õigusakti ellurakendamise käigus, siis tuleb koostada (täiendav) mõjuhinnang.

Kuidas toimida juba käimasolevate andmetöötlustoimingutega?

Üldmääruse kohane mõjuhinnang tuleb teha andmetöötlustoimingute osas, millega andmetöötleja alustab peale 2018. a. 25. maid ehk peale üldmääruse rakendumist.

Mõjuhinnang tuleb teha ka siis, kui andmetöötleja tänased isikuandmete töötlemise toimingud ja põhimõtted on alates 2018. a. 25. maist oluliselt muutunud. Näiteks on kasutusele võetud uus tehnoloogia, isikuandmete töötlemise eesmärgid on muutunud või isikute kohta tehtavate automaatsete otsuste ja profileerimiste osakaal andmetöötlemise protsessis on märkimisväärselt kasvanud.

6. peatükk. Kohustuslik eelkonsulteerimine

Vt. üldmääruse art. 36 ja pp. 94-96 ning direktiivi art. 28 ja pp. 59 ja IKS § 39.

Olete vastutava töötlejana teinud kavandatud andmetöötlusele andmekaitsealase mõjuhinnangu ja hinnanud ohte. Näete selle põhjal, et vaatamata kavandatud abinõudele ohtude vähendamiseks tooks uus andmetöötlus tõenäoliselt endaga kaasa suure ohu teokssaamise (nt. võimaldaks identiteedivargust, rahalist kahju, mainekahju, diskrimineerimist jne).[52] Sel juhul tuleb enne andmetöötlusega alustamist eelkonsulteerida Andmekaitse Inspektsiooniga.

Eelkonsulteerimise on sisuliselt teadaanne, et ettevõte/asutus on hinnanud oma andmetöötluse nii riskantseks, et peab tõenäoliseks suure ohu teokssaamist.

Kui andmetöötleja hindab, et ta saab andmetöötluse riske piisavalt maandada ning suure ohu realiseerumine ei ole tõenäoline, siis eelkonsulteerimise nõuet ei ole.

Eelkonsulteerimiseks tuleb inspektsioonile esitada läbiviidud mõjuhinnang. Mõjuhinnang peab andma selge pildi, milles seisneb suur oht, mida andmetöötleja ei suuda piisavalt maandada.

Kui vastav teave ei sisaldu ammendavalt juba mõjuhinnangus, tuleb mõjuhinnangule lisada:

- andmetöötlusega seotud vastutava(te) ja volitatud töötleja(te) omavahelised vastutusvaldkonnad;
- kavandatava andmetöötluse eesmärk ja vahendid;
- meetmed ja tagatised, kaitsmaks andmesubjekte;
- andmekaitsespetsialisti kontaktandmed, kui ta on määratud.

Inspektsioon annab andmetöötlejale kirjalikku nõu ning võib teha kohustavaid ja keelavaid ettekirjutusi.

Eelkonsulteerimine ei tähenda, et andmetöötleja vabaneb vastutusest. Kirjalik nõuanne ei tähenda, et inspektsioon muutuks tasuta audiitoriks, kes hindab ettevõtte/asutuse infosüsteemide ja dokumentatsiooni tugevusi ja nõrkusi ning soovitab konkreetseid parendusi. Kirjalik nõu võib olla lihtsalt üldine soovitus kavandatud andmetöötlusest hoiduda ja kaaluda veel võimalusi ohtude vähendamiseks.

[52] Suurt ohtu üritatakse näitliku loeteluna määratleda üldmääruse pp. 75 ja direktiivi pp. 51.

7. peatükk. Isikuandmetega seotud rikkumine. Oht (kahju)

Vt. üldmääruse art. 4 p. 12, art. 33, 34, pp. 75, 85-88; direktiivi art. 3 p. 11, art. 30, 31, pp. 61-62; IKS § 44, 45.
Vt. Euroopa andmekaitsenõukogu juhend „Suunised, mis käsitlevad isikuandmetega seotud rikkumistest teatamist määruse 2016/679 alusel"
Vrd küberturvalisuse seaduse küberintsidendist teatamise sätetega, eeskätt § 8.

Mis on rikkumine? Kellele tuleb sellest teatada?

Isikuandmetega seotud rikkumine on üldmääruse/direktiivi ning seda üle võtva IKS-i tähenduses turvanõuetega seotud rikkumine, mis põhjustab andmete:

- lubamatu hävimise, kaotsimineku või muutmise või
- lubamatu avalikustamise või lubamatu juurdepääsu võimaldamise.

Isikuandmetega seotud rikkumise korral kehtib andmetöötlejaile neli kohustust:
1) igasugune rikkumine tuleb dokumenteerida,

2) kui rikkumine põhjustas või tõenäoliselt põhjustab andmesubjektide õigustele ja vabadustele ohu (kahju), peab vastutav töötleja Andmekaitse Inspektsioonile rikkumisteate esitama;

3) kui rikkumine põhjustas või tõenäoliselt põhjustab andmesubjektidele suure ohu (suure kahju), peab vastutav töötleja sellest ka andmesubjektidele teada andma;

4) volitatud töötleja peab rikkumisest vastutavale töötlejale teada andma.

Täiendav, viies kohustus tuleb küberturvalisuse seadusest ja puudutab riigi- ja omavalitsusasutusi ning erasektorist üksnes elutähtsaid/olulisi teenusepakkujaid. Nemad peavad infosüsteemi turvalisust ohustavast olulisest küberintsidendist (nt. ründest arvutivõrgu vastu, pahavara kasutamisest) teatama Riigi Infosüsteemi Ametile.

Mida tähendab (suur) oht?

Isikuandmetega seotud rikkumisest teatamise kohustus sõltub sellest, mis on **oht andmesubjekti õigustele ja vabadustele**.

Andmekaitsespetsialisti määramise ja andmekaitsealase mõjuhinnangu tegemise kohustuse juures nimetavad üldmäärus ja direktiiv samuti **(suurt) ohtu**.[53] Selle juures peetakse silmas **riske**, mida põhjustab tundlik ja/või mahukas andmetöötlus. Näiteks seostame 5000 inimese terviseandmete või 50 000 inimese nö lihtandmete töötlemist suure ohuga (kõrge riskiga), mis tingib vajaduse määrata andmekaitsespetsialist ja teha mõjuhinnang.[54]

Rikkumisteatele seda kohaldada ei saa. Tõik, et ettevõtte kliendinimistusse on kogunenud üle 50 000 inimese andmed, ei ole ju rikkumine. Rikkumine on, kui nende andmetega juhtus või tõenäoliselt juhtub midagi halba:

> *Näide A: kaupluse klientide kodused ja e-posti aadressid said tehnilise vea või inimliku eksimuse tõttu avalikkusele nähtavaks.[55] Mõned väljaspool Euroopa Liitu asuvad ettevõtted kopeerisid need andmed ning hakkasid saatma rämpsposti. Otsene kahju seisneb rämpspostiga tülitamine. Tõenäoliselt*

[53] Üldmääruse art. 37 ja 35, direktiivi art. 32 ja 27, IKS § 40 ja 38.
[54] Käesoleva üldjuhendi 3. ja 5. ptk, kus defineeritakse suurt ohtu sisaldavat andmetöötlust.
[55] Võrdluseks: avalikus sektoris on eraisikute kontaktandmed juurdepääsupiiranguga teave ning selle lekkimise eest on ette nähtud väärteokaristus – vt avaliku teabe seaduse § 35 lg 1 p. 12 ja § 54^1.

oodatav lisaoht seisneb selles, et lekkinud andmete üle kadus kontroll, „mustalt" tegutsevad ettevõtted üritavad tõenäoliselt neid edasi müüa ning väljaspool Euroopa Liitu on raske nende tegevust tõkestada.

Näide B: lekkisid e-poe klientide kasutajanimed ja salasõnad. Tulemuseks on või tõenäoliselt võib olla, et keegi võõras teeb nende nimel ja arvel oste – see on otsese kahju oht inimese varale.

Näide C: retseptikeskuse infosüsteemi rikke tõttu ei saanud patsient apteegist talle määratud ravimit kätte. Kuigi järgmiseks päevaks oli rike kõrvaldatud, oli see isikuandmetega käideldavusega seotud rikkumine. Rikkumise definitsiooni mõttes oli tegu andmete ajutise kaotsiminekuga.[56]

Seega rikkumisteate esitamise kohustuse puhul peetakse ohu puhul silmas mitte üldist riski, vaid **reaalselt saadud või tõenäoliselt saadavat kahju**. Kahju tuleb siduda inimese **õiguste ja vabadustega**, näiteks:

- riive elule ja tervisele (haige ei saa infosüsteemi vea tõttu kätte talle määratud ravimit või veel hullem – saab vale ravimi),
- riive eraelule (kontaktandmed koos varasema ostuajalooga lekkisid, tulemuseks oli inimese profileerimine talle tundmatute isikute poolt, rämpspost ja kontrollimatu andmete edasimüümine),
- riive aule ja heale nimele (inimese kohta loodi tagaselja täiskasvanute portaali libakonto tema õigete kontaktandmetega, portaalis puudus konto loomisel kontroll, kas lisatud e-posti aadress ja telefoninumber on konto looja kontrolli all),
- vaba eneseteostuse ja ettevõtlusvabaduse takistus (inimese kohta levis piinlik väärinfo, mis ei lasknud tal edukalt ettevõtjana tegutseda),
- takistus tegevusala, elukutse ja töökoha valimise vabadusele (infosüsteemis hävisid inimese hariduskäigu kohta käivad andmed, mistõttu ta ei saanud õigel ajal kandideerida soovitud töökohale),
- riive omandi puutumatusele (salasõnade lekkimise tulemusena saadi juurdepääs inimese kasutajakontole ja tehti oste tema nimel ja arvel).

Rikkumisteate esitamise kohustus **ei olene sellest, kui mitut inimest või kui suuri andmemahte oht puudutab**.

Näide: kui veregrupp muutus tehnilise rikke tõttu infosüsteemis valeks või ei olnud kriitilisel hetkel kättesaadav, siis võib inimene operatsioonilauale sattudes selle pärast surra. Arvuliselt võttes puudutab see ühe inimese kohta käivat ühte tähemärki, kuid kahju oleks rängim, mis üldse juhtuda saab.

Suure ohu ja lihtsalt ohu eristamine sõltub kahju suurusest ehk tagajärje raskusest. Suur oht isikuandmetega seotud rikkumise mõttes on eelkõige:

- oht inimese elule, tervisele, varale ja mainele, aga samuti
- juhtumid, kus andmetöötluse probleemide tõttu ei saa inimene mingis ettevõtmises osaleda, kuhugi kandideerida, midagi taotleda, midagi tõendada. Isegi kui neid olukordi saab hiljem ilma otsese rahalise kuluta heastada, võib see tähendada arvestatavat aja-, töö- ja närvikulu.

Lihtsalt ohu näite alla kuuluvad need juhtumid, mis ei põhjusta märkimisväärt tagajärgi.

Näide A: infosüsteemi tõrge, mis ei lase aia- ja ehituskaupa müüva e-poe teenuseid kasutada ega omaenda ostuajalugu vaadata, on lihtne oht. Seevastu retseptikeskuse või e-tervise infosüsteemi tõrge on ilmselgelt suur oht.

[56] Vt. üldmääruse art. 4 p. 12, direktiivi art. 3 p. 11.

Näide B: kaupluse kolme kliendi ostuajaloo väljavõtted said inimliku eksituse tõttu kättesaadavaks võõrale isikule – üksnes tehtud ostud koos pärisnimest erinevate kasutajatunnustega. Võimalus, et võõras nende järgi suudab isikuid tuvastada, ei olnud konkreetseid asjaolusid arvestades tõenäoline. Seevastu ostuajaloo leke koos kliendi nime või kontaktandmetega või lausa koos salasõnadega on suur oht.

Tähele tuleb panna ka isikuandmetega seotud rikkumise ja küberintsidendi tähenduse erinevust:

1) isikuandmetega seotud rikkumine on seotud kahjuga inimese (nt. kliendi, töötaja, kodaniku) õigustele ja vabadustele. Kahju ettevõttele/asutusele endale ei puutu asjasse.

Näide: kaupluses avastati, et elektrooniline kliendiandmebaas on tehnilise rikke tõttu hävinud. Siiski õnnestus esialgu paberdokumentatsiooni kasutades tööd jätkata ning veidi hiljem varukoopiate ja paberdokumentide abil andmebaas taastada. Kauplusele tähendas see arvestatavat lisakulu, kuid kliente see ei mõjutanud. Vajadust rikkumisteate inspektsioonile saatmiseks ei ole.

2) küberintsident on seotud ohuga olulistele võrgu- ja infosüsteemidele ja nende teenustele.

Näide: küberturvalisuse seaduse mõttes olulist teenust pakkuva ettevõtte veebipõhist kliendiandmebaasi ei saanud võrguliikluse ründamise tõttu kasutada. Andmed ei lekkinud (neid ei saanud lihtsalt kasutada) ning teenuse pakkumist jätkati kohe ettevõtte tagavaraserveri pealt. Tegu oli olulise küberintsidendiga, kuid mitte isikuandmetega seotud rikkumisega. Kui aga teenuse osutamine oleks mõneks tunniks katkenud ning tegu on näiteks tervishoiu- või pangandusteenusega (mõju elule, tervisele või varale), siis tähendaks see ka andmekaitseliselt suurt ohtu.

Kuidas ohte hinnata ja vähendada? Näpunäiteid spetsialistile

Andmesubjekti õigustele ja vabadustele tekkiva ohu tõenäosus ja mõju tehakse kindlaks lähtudes andmetöötluse laadist, ulatusest, kontekstist ja eesmärkidest.[57] Ohtusid hinnataks objektiivse hindamise põhjal, millega tehakse kindlaks, kas andmetöötlustoimingutega kaasneb oht või suur oht.

Organisatsioonidele peaks ohu (riski) käsitlus olema tuttav nt IT- või kvaliteedijuhtimisest. Kui vaadata infoturvet, siis seni hinnati riske infovara käideldavusele, terviklusele ja konfidentsiaalsusele. Määrati riski allikad ja hinnati riski taset (kombinatsioonis tõenäosuse ja mõjuga). Riski hinnati mõjuna eelkõige organisatsioonile (varaline ja mainekahju).

Üldmääruse ohukäsitlus tähendab riskide hindamist isikule avalduva (tõenäolise) kahju seisukohast. Andmetöötleja, olles määranud riskid infovarale, peab nüüd lisaks hindama, milline on ohu teokssaamisel isikule tekkiv võimalik kahju. Määratakse riski tase isikule, nt skaalal *madal, keskmine, kõrge*. Valitakse meetmed riskide haldamiseks ja aktsepteeritakse jääkrisk.

Toome ka mõned näited meetmetest, mille abil ohte vähendada:

- andmeid kogutakse ja kasutatakse minimaalselt (nii vähe kui võimalik) ja säilitatakse üksnes seniks, kuni neid vajatakse;
- piiratakse andmetele juurdepääsu (nii organisatsiooni siseselt kui väliselt);
- tagatakse korrapärane isikuandmete kustutamine pärast säilitustähtaja lõppemist;
- kasutatakse krüptimist, pseudonüümimist, anonüümimist;
- andmeid töödeldakse piiratud juurdepääsuga ruumides;
- rakendatakse uuemaid ja kaasaegsemaid infotehnilisi turvameetmeid;
- koolitatakse töötajaid ja koostööpartnereid;

[57] Vt käesoleva üldjuhendi lisa 4.

- luuakse lahendusi, kus isikud saavad kergemini oma andmetele ligi (nt e-teenindus);
- läbipaistvad kasutustingimused, mis annavad ka isikule endale võimaluse enda turvalisuse eest paremini seista.

Kuidas toimub rikkumiste dokumenteerimine?

Vastutav töötleja peab dokumenteerima kõik isikuandmetega seotud rikkumised:

- millised on rikkumise asjaolud,
- milline on rikkumiste mõju füüsilistele isikutele ning
- milliseid parandusmeetmeid (nt tehnilised, korralduslikud) vastutav töötleja rakendab kahjustatud isikuandmete suhtes.

Kui aga rikkumisega seotud ohtu (kahju) pole, siis inspektsioonile rikkumisteadet esitada ei ole vaja. Toome mõned näited:

Näide A: ettevõttes toimus kliendihaldustarkvara uuendus. Juurdepääs erinevatele kliendiandmetele oli ettevõttesiseselt reguleeritud ja piiratud. Peale tarkvarauuendust avastas üks töötajatest, et ta nägi klientide kohta nüüd rohkem andmeid kui pidanuks. Töötaja informeeris sellest tööandjat. Viga sai kiirelt likvideeritud. Tegu on isikuandmetega seotud rikkumisega (konfidentsiaalsuse rikkumine), mis tuleb dokumenteerida. Kuid et rikkumine avastati kohe ning klientidele ohtu ei olnud, siis inspektsioonile teatama ei pea.
Näide B: ettevõtte töötaja sõidukist varastati sülearvuti, milles olid messil kogutud potentsiaalsete uute klientide isikuandmed. Sülearvuti kõvaketas oli ajakohaselt krüpeertitud. Tegu on isikuandmetega seotud rikkumisega (käideldavuse rikkumine), mis tuleb dokumenteerida. Ohtu isikutele aga ei ole (andmed krüpteeritud), seega inspektsioonile teatama ei pea.
Näide C: haiglat tabas lunavararünne. Blokeeriti juurdepääs osade patsientide terviseandmetele. Haigla varundas korrapäraselt andmeid. Varundatu jäi ründest puutumata. Andmete taastamine varukoopiatelt võttis aega kolm tundi. Tegu on suure ohuga – arstidel ei olnud ajakriitilise ravi puhul võimalik patsientide terviseandmeid vaadata (veregrupid, allergiad, varasem ravi). See tuleb dokumenteerida (käideldavuse, tervikluse, konfidentsiaalsuse rikkumine). Teatada tuleb nii inspektsioonile, Riigi Infosüsteemi Ametile (küberintsident) kui andmesubjektidele.

Millal ja kuidas tuleb rikkumisest teatada inspektsioonile?

Vastutav töötleja teatab inspektsioonile põhjendamatu viivituseta, võimaluse korral **72 tunni jooksul** pärast rikkumisest teada saamist, mis põhjustas või tõenäoliselt põhjustab ohu andmesubjektidele.

Isegi kui kõik rikkumise põhjused ei ole veel teada või pole lõplikult selge näiteks rikkumist puudutavate isikute arv, tuleks esmane teade 72 tunni jooksul siiski teha.

See annab inspektsioonile võimaluse rikkumise olemust varakult hinnata ning anda andmetöötlejale vajadusel tagasisidet ja soovitusi.

Täiendavate asjaolude ilmnemisel edastab andmetöötleja need põhjendamatu viivituseta jätkuteavitusena. Andmetöötleja peab põhjendama, miks ei olnud esialgses teatises võimalik kõiki rikkumist puudutavaid asjaolusid anda.

Kui rikkumise tuvastab isikuandmete volitatud töötleja, teavitab ta sellest põhjendamatu viivituseta vastutavat töötlejat, kes omakorda teavitab siis järelevalveasutust.

Inspektsioonile edastatud rikkumisteade peab sisaldama:

- isikuandmetega seotud rikkumise laadi kirjeldust. Selleks võib olla näiteks andmete kaotsiminek või hävimine, vargus, koopia tegemine. Samuti volituseta muutmine, lugemine või edastamine;
- võimaluse korral asjaomaste andmesubjektide kategooriaid ja nende ligikaudne arv ning isikuandmete asjaomaste kirjete liike ja ligikaudset arvu;
- andmekaitsespetsialisti või muu kontaktisiku nime ja kontaktandmeid;
- isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldust;
- meetmete kirjeldust isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

Inspektsioon on koostanud rikkumisteate täpsema vormi valikvastustega. Vorm on kättesaadav inspektsiooni võrgulehel.

Üldkasutatava elektroonilise sideteenuse osutaja suhtes kehtis rikkumisteate esitamise kohustus juba varem. Nende teadete nõuded ja sisu on kehtestatud Euroopa Komisjoni määrusega (EL) 611/2013.

Millal ja kuidas peab rikkumisest teatama andmesubjektile?

Kui rikkumise tulemusena tekib inimeste õigustele ja vabadustele tõenäoliselt **suur oht**, peab vastutav töötleja põhjendamatu viivituseta sellest teavitama ka andmesubjekti.

Teavituse eesmärk on lisaks andmetöötlejale võimaldada ka andmesubjektil endal võtta vajalikke ettevaatusabinõusid ohu leevendamiseks (näiteks salasõna muutmiseks).

Teates tuleb kirjeldada isikuandmetega seotud rikkumise olemust, samuti tuleks anda soovitusi võimaliku kahjuliku mõju leevendamiseks.

Isikule edastatavas teates peavad olema:

- selges ja lihtsas keeles selgitatud isikuandmetega seotud rikkumise olemus;
- andmekaitsespetsialisti või muu kontaktisiku nimi ja kontaktandmed;
- isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldus;
- meetmete kirjeldus isikuandmetega seotud rikkumise lahendamiseks.

Otsese ohu leevendamise vajadus eeldaks andmesubjekti kohest teavitamist, samal ajal kui vajadus rakendada asjakohaseid meetmeid rikkumiste jätkumise või samalaadsete rikkumiste ärahoidmiseks võib õigustada hilisemat teavitamist.

Andmesubjekti teavitamist ei nõuta, kui:

- vastutav töötleja oli juba rakendanud kohaseid kaitsemeetmeid ja neid juba kohaldati rikkumisest mõjutatud isikuandmetele (eelkõige andmete kõrvalistele isikutele kättesaamatuks muutmine, näiteks olid lekkinud andmed krüpteeritud);
- vastutav töötleja rakendas hilisemad meetmed, mis tagavad, et suure ohu teke ei ole enam tõenäoline, või
- teavitamine nõuaks ebaproportsionaalseid jõupingutusi. Sellisel juhul tehakse avalik teadaanne või võetakse muu sarnane meede, millega teavitatakse andmesubjekte tulemuslikul viisil.

Kui andmetöötleja ei pea vajalikuks andmesubjekte teavitada, on inspektsioonil siiski õigus vastutavalt töötlejalt andmesubjektidele teatamist nõuda.

Kokkuvõtvalt saab öelda, et rikkumiste haldamine nõuab andmetöötlejalt ettevalmistustööd. Tuleb kaardistada kõik protsessid ning ohud (organisatsioonisisesed kui välised). Iga ohu puhul tuleb hinnata, kas ja milline mõju on andmesubjektile. Nii on rikkumise toimumisel võimalik kiirelt reageerida, sh otsustada inspektsioonile ja andmesubjektidele teatamise vajadus.

8. peatükk. Andmete ülekandmine

Vt. üldmääruse art. 20 ja pp. 68.
Vt. Euroopa andmekaitsenõukogu „Suunised andmete ülekandmise õiguse kohta".

Mida tähendab andmete ülekandmine?

Õigus tutvuda enda kohta käivate andmetega on Euroopa Liidu/Ühenduse liikmesriikides kehtinud aastast 1995 saadik. Isikuandmete kaitse üldmäärus tõi selle kõrvale **õiguse nõuda andmete ülekandmist**. Esimene neist on laiem (ligipääs mistahes alusel kogutud ja mistahes kujul hoitavatele andmetele, sh nt paberandmetele). Teine on kitsam (üksnes digitaalandmed, mis kogutud lepingu või nõusoleku alusel).

Õigus nõuda andmete ülekandmist tähendab, et inimene võib küsida ja saada vastutavalt töötlejalt kõiki **teda** puudutavaid isikuandmeid, mida ta on andmetöötlejale **edastanud.** Seda kõike

- struktureeritud, üldkasutatavas vormingus ning
- masinloetaval kujul.

Samuti on inimesel õigus saadud andmed edastada teisele andmetöötlejale kas ise või paluda seda teha andmetöötlejal, kellelt andmed saadi.

Mis on ülekandmisõiguse eesmärk? Silmas peeti nii paremat kontrolli oma andmete üle (inimestel on lihtne oma isikuandmeid hallata ja taaskasutada) kui ka konkurentsi edendamist andmemajanduses (inimene saab oma andmetega minna ühe teenusepakkuja juurest teise juurde).

Andmetöötleja peab inimest temaga seotud andmete ülekandmise õigusest informeerima.[58]

Mis on edastatud andmed?

Edastamisena tuleb käsitleda kõiki andmeid, mida inimene edastab andmetöötlejale

- otseselt kas ise (näiteks sisestab enda kohta andmed kasutajakonto avamisel) või
- edastatakse teenuse tarbimise (näiteks poes ostude sooritamise, nutiseadme kasutamise) käigus.

Edastatud andmete põhjal võib aga andmetöötleja ise luua täiendavaid andmeid – näiteks profileerides inimese eelistusi ja harjumusi. See täiendav analüütiline andmestik ei kuulu edastatud andmete hulka. Inimesel on küll õigus nõuda sellega tutvumist (aluseks üldmääruse art. 15), kuid mitte ülekandmist (üldmääruse art. 20).

Mis alusel loodud andmeid saab üle kanda?

Andmete ülekandmist saab kohaldada ainult nendele andmetele, mille kogumise aluseks on kas inimese **nõusolek** või inimese ja andmetöötleja vahel sõlmitud **leping.**

[58] Vt üldmäärus art. 13 lg 2 p. b, art. 14 lg 2 p. c.

Seega on ülekantavuse kohaldumisalas andmed, mida inimene andis enda kohta (nt nimi, kasutajatunnus, kontaktandmed, enda märgitud eelistused jms) ning mis tekkisid tema tegevuse käigus:

- ostuajalugu kaupluses;
- elektri, gaasi ja vee tarbimise ajalugu elektri- või gaasimüügi või ühisveevärgi ettevõttes;
- nutirakendusse tekkinud andmed rakenduse kasutaja tegevuste kohta;
- hambaarsti juurde tekkinud andmed hambaravi kohta.

Kui andmetöötlus toimub avaliku võimu teostamisel, avaliku ülesande täitmisel (seaduse alusel), siis õigus andmete ülekandmisele ei kohaldu. See on ka põhjus, miks õiguskaitseasutuste andmekaitsedirektiiv ning seda üle võttev IKS andmete ülekantavuse õigust ei tunne – õiguskaitsevaldkonnas ei koguta isikuandmeid lepingu või nõusoleku alusel.

Samuti ei kohaldu ülekantavus andmetele, mida ettevõte või asutus töötleb üksnes seadusejärgse kohustuse täitmiseks – näiteks maksuarvestuseks või raamatupidamiseks. Kuid samad andmed võivad ettevõttes olla korraga kahel alusel – lepingu täitmiseks ja ühtlasi raamatupidamiseks.

Mis vorminõudeid tuleb andmete ülekandmisel järgida?

Andmete ülekandmise õiguse tagamiseks peab vastutav töötleja isikuandmed edastama:

- struktureeritult, üldkasutatavas vormingus ning
- masinloetaval kujul.

Et andmetöötlejal oleks võimalik nimetatud vorminõudeid täita, seab üldmäärus lisatingimuse, mille kohaselt kuuluvad ülekandmisele ainult need isikuandmed, mida andmetöötleja töötleb automatiseeritult. Näiteks paberkandjatel olevad isikuandmed siia alla ei kuulu.

Üldkasutatava ehk avatud vormingu all peetakse silmas vorminguid, mis ei ole seotud kitsamalt kasutatava kommertstarkvaraga.

Masinloetav kuju tähendab oma olemuselt struktureeritud faili, millest tarkvararakendused suudavad spetsiifilisi andmeid, sh üksikuid faktiväiteid ja nende sisemist struktuuri (metaandmeid), kergelt tuvastada, ära tunda ja välja lugeda.

Masinloetavad avatud vormingud on näiteks XML (***Ex**tensible **M**arkup **L**anguage* – laiendatav märgistuskeel)', JSON (***J**ava**S**cript **O**bject **N**otation* – lihtsustatud andmevahetusvorming), CSV (**c**omma-**s**eparated **v**alue – piiritletud tekstifail, kus välju/väärtusi eraldatakse koma abil).

Samuti saab inimene nõuda, et üks andmetöötleja edastab andmed otse teisele andmetöötlejale. Seda siis juhul, kui see on **tehniliselt teostatav**. See tähendab, et kui inimene soovib näiteks vahetada e-posti, panga- või kõneteenuse pakkujat, on tal õigus nõuda, et senine teenusepakkuja edastab tehnilisel võimalusel inimesega seotud isikuandmed otse uuele teenusepakkujale.

Kas andmetöötleja peab peale andmete ülekandmist andmed kustutama?

Ei, see ei tähenda, et inimene peab oma kliendisuhte senise teenusepakkujaga lõpetama. Ülekandmine võib olla andmete kopeerimine – klient jagab ühe teenusepakkuja juures olevaid andmeid teise teenusepakkujaga ning on samaaegselt mõlema klient. Tõsi, ülekandmine võib ka tähendada, et kliendisuhe lõpeb ja eelmise teenusepakkuja juurest andmed kustutatakse, kui muud alust nende säilitamiseks enam ei ole.

Senine teenusepakkuja ei pea ülekandmise järel kõik inimesega seotud isikuandmed kustutama (isegi kui kliendisuhe lõpeb). Nõuded andmete säilitustähtaegadele võivad tulla nii eriseadustest või ka lepingust (lepingu tüüptingimustest). Näiteks kauplus säilitab (endise) kliendi andmeid sisaldavaid raamatupidamise algdokumente raamatupidamisseaduse § 12 alusel seitse aastat

Kuidas tagada ülekandmisel teiste isikute õiguste kaitse?

Tihti on inimesega seotud andmetöötlustoimingutesse kaasatud ka teised isikud. Näiteks tehes pangaülekannet, helistades või ühismeedias suheldes on meie tegevusse hõlmatud ka teised osapooled, kes saavad või saadavad raha või kellega me suhtleme.

Andmete ülekandmise raames ei tohi kahjustada teiste isikute õigusi ja vabadusi. Teise isiku all tuleb mõista nii füüsilist isikut kui ka näiteks äriühingust andmetöötlejat koos tema valduses oleva intellektuaalomandi või ärisaladusega.

Näiteks kui inimene on e-posti teenuses salvestanud sõprade, tuttavavate või sugulaste kontaktandmed ning palub olemasoleval teenusepakkujal need edastada uuele teenusepakkujale, võib viimane neid andmeid töödelda ainult algsel eesmärgil, milleks on kontaktandmete säilimise tagamine. Sama kehtib ka inimese maksetehingute ajalooga, mis kantakse olemasolevast pangast uude. Nii uus pank kui e-posti teenusepakkuja ei tohi pangatehingus osalenud teiste inimeste andmeid või e-posti kontaktide nimekirja automaatselt kasutada näiteks oma teenuse pakkumiste või muude otseturustussõnumite edastamiseks.

Mis aja jooksul tuleb isiku andmete ülekandmise taotlusele vastata?

Taotlusele tuleb vastata põhjendamatu viivituseta, kuid mitte hiljem kui ühe kuu jooksul pärast taotluse saamist. Vajaduse korral võib andmetöötleja ajavahemikku pikendada kahe kuu võrra. Kuid sellisest pikendamisest tuleb anda ühe kuu jooksul isikule teada.

Näiteks võib selguda, et andmetöötleja peab andmekoosseise eelnevalt puhastama, et välistada teiste isikute õiguste rikkumine. Puhastamine on ajamahukas töö. Sel juhul annab andmetöötleja taotlejale sellest viivitamatult teada ja ütleb uue tähtaja. See peab jääma maksimaalselt kolme kalendrikuu piiresse.

Seega eeldab andmete ülekantavus vastutavatelt töötlejatelt täiendavat andmetöötluse kihti, et andmeid platvormilt kätte saada ja eraldada ülekantavuse kohaldamisalast väljapoole jäävad isikuandmed, nagu kaudsed andmed või süsteemide turvalisusega seotud andmed. Seda täiendavat andmetöötlust peetakse põhilise andmetöötluse kõrvaltoiminguks, sest seda ei tehta vastutava töötleja määratletud uue eesmärgi saavutamiseks.

Kui andmetöötleja keeldub ülekandmistaotlust rahuldamast, on ta kohustatud isikule ühe kuu jooksul selgitama keeldumise põhjuseid.

9. peatükk. Nõusoleku küsimine

Vt. üldmääruse art. 4 p. 11, art. 6-9 ja pp. 27, 32, 33, 38, 40, 42, 43, 50.
Vt. Euroopa andmekaitsenõukogu suunist „Suunised määruse 2016/679 kohase nõusoleku kohta"

Mis on nõusolek?

Nõusolek üldmääruse tähenduses on andmesubjekti

- vabatahtlik,
- konkreetne,
- teadlik,
- ühemõtteline

tahteavaldus, millega ta kas

- avalduse vormis või
- selget nõusolekut väljendava tegevusega

nõustub enda kohta käivate isikuandmete töötlemisega.

Õiguskaitseasutuste andmekaitsedirektiivi kohaldamisalas (vt IKS 4. peatükk) nõusolekut ei kasutata.

Millal on nõusolek asjakohane?

Isiku nõusolek on üks kuuest võimalikust õiguslikest alustest isikuandmete töötlemiseks.[59] Kui nõusoleku küsimine ei vasta üldmääruses ettenähtud tingimustele, tuleb andmete töötlemiseks leida muu õiguslik alus või neid mitte töödelda.

Nõusolek on vabatahtlik tahteavaldus, mida inimene võib ka igal ajal vabalt tagasi võtta. Selle küsimine on asjakohane vaid sellises olukorras, kus isikul on ka reaalselt võimalik otsustada oma isikuandmete töötlemise üle.

Väär on küsida nõusolekut olukorras, kus tegelikult on isikuandmete töötlemiseks muu õiguslik alus. Taoline tegevus on eksitav, jättes mulje, et inimesel on otsustusõigus olukorras, kus seda tegelikult ei ole.

Tuleb hoiduda nõusoleku mõiste kasutamisest seal, kus inimesele antakse lihtsalt teada lepingu alusel andmetöötlusest ettevõttes (või lepingu või tüüptingimuste muutumisest). Samuti peavad asutused hoiduma nõusoleku mõiste kasutamisest seal, kus nad tegelikult vaid informeerivad inimest avaliku võimu teostamise või avaliku ülesande täitmise käigus toimuvast andmetöötlusest.

Üldmääruse mõttes ei ole nõusolekuga tegu ka väljapoole üldmääruse kohaldamisala jäävates tegevustes. Näiteks ei kohaldata üldmäärust juhul, kui isikuandmeid töödeldakse isiklikul otstarbel.

Näide: lasteaiapeol laste pildistamine isikliku fotoalbumi tarbeks on isikuandmete töötlemine isiklikul otstarbel. Sel juhul ei kohaldata üldmäärusest tulenevaid nõudeid, sh nõusoleku osas. See ei välista heast kasvatusest tulenevat viisakust pildistamiseks pildistatava nõusolemist küsida.

[59] Üldmääruse art. 6 kohaselt on isikuandmete töötlemise aluseks kas 1) isiku nõusolek, 2) lepingu täitmine või sõlmimise ettevalmistamine, 3) seadusejärgne kohustus, 4) eluliste huvide kaitse, 5) avaliku võimu teostamine, avaliku ülesande täitmine, 6) õigustatud huvi.

Nõusolekut ei pea võtma olukorras, kus ettevõte/asutus tegelikult inimesi ei tuvasta ega saakski mõistlike pingutustega tuvastada. Näiteks on paljud veebiteenused sellised, kus kasutajaid ei tuvastata ei reaalse ega väljamõeldud identiteedi alusel ega viia profileerimiseks kokku samalt IP-aadressilt tulnud erinevaid võrgulehe külastusi. Sellisel juhul ei pea hakkama inimest vastu tema tahtmist tuvastama, et talt andmete töötlemise nõusolek võtta.[60]

Kas avalikus sektoris võib töödelda isikuandmeid nõusoleku alusel?

Kui isikuandmete töötlemine toimub avaliku võimu teostamise või avaliku ülesande täitmise käigus, ei ole andmetöötlejal õigust küsida isikult lisaks ka nõusolekut samade andmete töötlemiseks. Selline olukord on isikut eksitav ega vasta üldmääruse tingimustele.

See ei tähenda, et avaliku sektori asutuste andmetöötlusest on nõusolek kui õiguslik alus välistatud. Nõusoleku alusel võib isikuandmeid töödelda selliste juhtumite puhul, kus tõesti isikul on õigus otsustada oma andmete töötlemise üle kartmata kahjulikke tagajärgi. Nõusoleku annab isik vabatahtlikult ja võib selle igal hetkel tagasi võtta. Selliseks olukorraks võib pidada eeskätt mugavusteenuseid.

> *Näide: vallavalitsus planeerib teeremonti, mida viiakse läbi pikema aja vältel ning mis häirib tugevalt liiklust. Vallavalitsus pakub välja võimaluse isikutel liituda meililistiga, et saada teavitusi teeremondi ja liiklusseisakute kohta. Sama info on esitatud ka omavalistuse võrgulehel. Taoline kirjavahetus toimub nõusoleku alusel ning isikul on igal ajal võimalus kirjade saamisest loobuda. Isik, kes ei soovi elektroonilisi teavitusi, ei jää samas siiski infost ilma ja võib seda igal ajal võrgulehelt vaadata.*

Millal on nõusolek kehtiv?

Nõusolek on vabatahtlik tahtveavaldus, millega isik teadlikult lubab oma isikuandmete töötlemist. Nõusolekut ei loeta vabatahtlikult antuks, kui isikul puudub vaba valikuvõimalus või ta ei saa nõusoleku andmisest kahjulike tagajärgedeta keelduda või seda tagasi võtta. Nõusolek ei ole antud vabatahtlikult, kui näiteks teenust ostes puudub valikuvõimalus elektroonilise reklaami saamise osas (*„Me ei sõlmi Teiega seda lepingut, kui Te ei ole nõus meilt edaspidi uudiskirju ja soodsaid pakkumisi saama!“*).

Sama kehtib ka olukorras, mil isikul puudub võimalus anda **nõusolek iga andmetöötluse eesmärgi puhul eraldi**.

Nõusolekut ei loeta vabatahtlikult antuks olukorras, kus inimene ja andmetöötleja on selgelt ebavõrdses olukorras (eriti avaliku sektori asutuse puhul või töösuhetes) ning on vähetõenäoline, et isik andis konkreetses olukorra nõusoleku vabatahtlikult.

Nõusoleku kehtivusele ei ole etteantud konkreetset ajalist tähtaega. Nõusoleku ajaline kehtivus sõltub andmete töötlemise tingimustest ja eesmärkidest. Seega tuleks andmetöötlejal eelnevalt antud nõusolekute asjakohasust aeg-ajalt uuesti hinnata. Andmete vastutav töötleja peab silmas pidama, et nõusoleku tõendamise kohustus lasub just temal. Kui andmete töötlemise eesmärgid, mahud ja muud tingimused muutuvad, siis ei ole eelnevalt antud nõusolek kehtiv ning tuleb küsida uus nõusolek.

Küll aga võib isik nõusoleku igal ajal tagasi võtta. **Nõusoleku tagasivõtmise võimalusest tuleb isikut informeerida** (nõusoleku vormis ja andmekaitse tingimustes) juba enne nõusoleku võtmist ning tagasivõtmise protseduur peab olema sama lihtne kui selle andmine. Nõusoleku

[60] Vt üldmääruse art. 11.

tagasivõtmine ei mõjuta nõusoleku alusel toimunud andmete töötlemise seaduslikkust. Kui isik võtab oma nõusoleku tagasi, tuleb tema andmete töötlemine lõpetada.

Millised on nõuded nõusoleku sisule ja vormile?

Nõusolek peab olema selgesõnaline ja konkreetne kinnitus kirjalikus, elektroonilises või suulises vormis. Nõusoleku sõnastus peab olema lihtsas ja arusaadavas sõnastuses ning kergesti kättesaadav.

Nõusoleku sõnastamisel tuleb arvestada ka sihtgrupiga, kellelt nõusolekuid küsitakse, nt alaealiste puhul peaks olema sõnastus arusaadav ka alaealisele.

Vaikimist, eeltäidetud (märgistatud) lahtreid ning tegevusetust ei loeta nõusoleku andmiseks.

Nõusoleku vormis peab olema teave selle kohta, kes on **isikuandmete töötleja** ning millisel **eesmärgil** isikuandmeid töödeldakse. Lisaks tuleb inimesele teatada võimalusest nõusolek tagasi võtta.

Olenevalt konkreetsest olukorrast ning nõusoleku küsimise viisist ei ole keelatud nõusoleku vormis esitada täpsemat ülevaadet andmetöötlustingimuste, sh isiku muude õiguste kohta. Kui töödeldakse lisaks ka **eriliigilisi** andmeid,[61] siis peab see olema nõusoleku vormis selgelt välja toodud.

Kui nõusolekut küsiv dokument hõlmab ka muid küsimusi (näiteks lepingu teksti), siis peab nõusolek olema selgelt eristatav. **Kui andmeid küsitakse nii nõusoleku alusel kui ka muudel alustel** (nt seadusejärgne kohustus, lepingu sõlmimiseks või täitmiseks), **siis peab andmeid esitades olema selgelt arusaadav, milliseid andmeid on kohustuslik esitada** (nö tärniga märgistatud väljad) **ja milliste andmete esitamine on vabatahtlik** (nõusoleku alusel esitatavad). **Kui andmete töötlemisel on mitu eesmärki, tuleb iga eesmärgi osas eraldi nõusolek anda.**

> Näide: Isik soovib osaleda elektroonilises uuringus tema käitumisharjumuste kohta. Korrektne ja lihtsas sõnastuses nõusoleku küsimine oleks sellisel juhul:
>
> *Uuringufirma X korraldab uuringu, millega soovitakse kaardistada igapäevaseid sportimisharjumusi. Uuringu tulemused esitatakse anonüümse üldistatud kokkuvõttena.*
>
> *Uuringus osalemise nõusoleku võite igal ajal tagasi võtta. Täpsemalt nõusoleku tagasivõtmise ja uuringu enda kohta saate lugeda siit (link lehele).*

> ☐ *Soovin osaleda sportimisharjumuste uuringus ning olen nõus uuringu jaoks oma andmete töötlemisega.*

> Nõusoleku andmiseks peab isik kasti tegema linnukese. Sellise näite puhul on väär kasutada isikuandmeid hiljem näiteks reklaami edastamiseks, kuna reklaami saatmiseks ei ole selle sõnastuse kohaselt nõusolekut küsitud.

Kuna nõusoleku olemasolu peab tõendama vastutav töötleja, siis peab nõusolekuid alles hoidma vähemalt andmete töötlemise lõpuni ning pidama nende aja- ja asjakohasuse osas arvestust.

Andmetöötleja peab arvestama, et **isikul on õigus igal ajal nõusolekut tagasi võtta** ning see peab toimuma sama lihtsal viisil, kui nõusoleku andmine. Nõusoleku tagasivõtmine ei mõjuta enne

[61] Eriliigilised andmed on loetletud üldmääruse artiklis 9

tagasivõtmist nõusoleku alusel toimunud andmetöötluse seaduslikkust. Andmetöötleja peaks eelnevalt analüüsima ka tagasivõtmise viise ja võimalusi. Näiteks pakkuma oma võrgulehel vastavat vormi või võimaldama seda teha telefonitsi (näiteks juhul, kui algne nõusolek küsiti ka telefonitsi).

Nõusoleku küsimiseks ja paremaks haldamiseks koostasime kontrollküsimustiku – vt käesoleva üldjuhendi lisa 2.

Mida peab teadma alaealise isikuandmete töötlemisest?

Laste isikuandmed vajavad töötlemisel erilist kaitset, kuna laps ei pruugi täielikult mõista andmetöötlusega kaasnevaid ohtusid, tagajärgi ja kaitsemeetmeid. Seepärast annab alaealise andmete töötlemiseks nõusoleku tema lapsevanem või eestkostja.

Erand on lapse nõusolekule ettenähtud seoses infoühiskonna teenuste (Interneti vahendusel kasutatavad teenused) osutamisega. Nimelt, kui pakutakse infoühiskonna teenust nõusoleku alusel, siis on alaealise andmete töötlemine seaduslik vaid juhul, kui laps on vähemalt 13-aastane.[62]

Seega alates sellest vanusest on alaealisel endal otsustusõigus ehk nõusoleku andmise õigus infoühiskonna teenuse saamiseks. Alla selle vanusepiiri annab lapse eest nõusoleku lapsevanem või eestkostja. Oluline on silmas pidada ka seda, et lapsevanema või eestkostja antud nõusolek kehtib lapse täiskasvanuks saamisel edasi. Kui laps on saanud täiskasvanuks, siis on tal näiteks võimalus lapsevanema või eestkostja antud nõusolek tagasi võtta või seda muuta.

Kui laps kasutab alaealistele suunatud *on-line* ennetus- või nõustamisteenust (nt lasteabi teenus), siis selleks ei ole vaja lapsevanema või eestkostja eelnevat nõusolekut.

Mida peab teadma nõusolekust pärast isiku surma?

Üldmäärus ei kohaldu surnu andmetele. Liikmesriikidel on siiski õigus surnu kaitseks (ja temaga seotud elavate kaitseks) andmekaitsereegleid kohaldada.[63]

Eesti isikuandmete kaitse seadus on kehtestanud selles osas järgmised reeglid:

Isiku antud nõusolek kehtib tema eluajal ja 10 aastat pärast tema surma juhul, kui isik ei ole otsustanud teisiti. Kui isik suri alaealisena, siis kehtib tema antud nõusolek 20 aastat pärast tema surma.

Kui ilmneb, et isikuandmeid on vaja töödelda pärast isiku surma, siis saab selleks nõusoleku anda surnud isiku pärija. Kui pärijaid on mitu, võib nõusoleku anda ja selle ka tagasi võtta ükskõik milline neist pärijatest.

Kui töödeldakse vaid surnud isiku nime, sugu, sünni- ja surmaaega, surmafakti ning matmise aega ja kohta, siis ei ole pärija nõusolekut vaja.

Seega võib ilma pärija nõusolekuta isikuandmeid töödelda järgnevatel juhtudel:

- töödeldakse isikuandmeid, mille töötlemiseks ei ole vaja nõusolekut;

---

[62] Üldmääruse art. 8 sätestab üldreeglina vanusepiiriks 16 aastat, lubades liikmesriikidel seda vanust langetada kuni 13 aastale. Eesti isikuandmete kaitse seadus kehtestab vanusepiiriks 13 aastat.
Rahvusvahelisest taustast niipalju, et USA laste e-privaatsuse seadus (*Children's Online Privacy Protection Act*) kehtestas 13-aasta reegli juba aastal 1998.

[63] Vt. üldmääruse pp. 27.

- isikuandmete töötlemine toimub muudel õiguslikel alustel;
- isiku surmast on möödunud rohkem kui 10 aastat;
- alaealiselt surnud isiku surmast on möödunud 20 aastat.

Lisaks eeltoodule tuleb ka arvestada võimalusega, et valdkondlikes seadustes võivad olla ka lisatingimused, millal võib surnud isikute andmeid töödelda. Näiteks peavad avaliku teabe seaduse kohased teabevaldajad arvestama ka sama seaduse § 40 lõikega 3.

10. peatükk. Läbipaistvus

Vt. üldmääruse art. 5 lg 1 p. a ja lg 2, art. 12-22, pp. 39, 58-72.
Vt. Euroopa andmekaitsenõukogu „Suunised määruse 2016/679 läbipaistvuse kohta"

See peatükk käsitleb üldmääruse, mitte direktiivi kohaldamist

Antud peatükis käsitletakse isikuandmete töötlemise läbipaistvuse nõuet üldmääruse kohaldamisalas. Üldmäärus on läbipaistvuse toonud esmakordselt andmekaitse aluspõhimõtete hulka.

Õiguskaitseasutuste andmekaitsedirektiivi aluspõhimõtete hulgas läbipaistvust ei ole.[64] Kuigi suur osa üldmääruse läbipaistvusnõuetest on leitav ka direktiivist, on nende ulatus üldmäärusega võrreldes mõnevõrra väiksem ning liikmesriigi seadusandjal mõnevõrra vabamad käed. Õiguskaitsevaldkonna eripära arvestades on see ka mõistetav.

Seetõttu ei käsitleta selles peatükis direktiivi läbipaistvusnõudeid – inimeste teavitamist õiguskaitseasutuste poolt süütegude tõkestamisel, avastamisel, menetlemisel ja karistuste täideviimisel. Sellistel juhtudel on teavitamise sisu ja kord ettenähtud Eesti isikuandmete kaitse seaduses (vt § 22 ja § 23) ning menetlusseadustikes.

Mida üldse tähendab läbipaistvus?

Andmekaitsealase läbipaistvuse võib kokku võtta järgmiselt:

1) inimesele tuleb siis, kui temalt andmeid kogutakse, anda andmetöötleja ja andmetöötluse kohta teavet;
2) seda tuleb teha ka siis, kui andmed ei ole saadud temalt endalt (v.a. kui teatamine oleks ebaproportsionaalselt keeruline või on andmete saamine või salajas hoidmine seadusega ette nähtud);
3) inimesel on enda kohta käivate andmete osas:
    a. õigus tutvuda oma andmetega,
    b. asjakohasel juhul õigus nõuda andmete parandamist, kustutamist, töötlemise piiramist, andmete ülekandmist, samuti õigus esitada vastuväiteid ja keelata otseturundust,
    c. kaitse masina tehtud otsuste vastu (v.a. lepingu ja seaduse alusel otsustamisel);
4) kõigest eelnevast tuleb inimesele teada anda kokkuvõtlikult, selgelt ja arusaadavalt, lihtsasti kättesaadavas vormis, reeglina kuu aja jooksul ja reeglina tasuta.

Eelnevate nõuete täitmiseks on vastutaval töötlejal hädavajalik koostada ja avaldada oma **andmekaitsetingimused** – sarnaselt kliendilepingute üld- või tüüptingimustega.

Lisaks kindlustab läbipaistvust ka andmetöötleja kohustus anda suure ohu korral inimesele teada tema andmetega toimunud rikkumisest.

Andmekaitsetingimused – teave, mida peab andmetöötluse kohta andma

Vastutav töötleja avaldab inimesele tema andmete töötlemise kohta järgmise teabe (andmekaitsetingimused):[65]

[64] Vrd. üldmääruse art. 5 lg 1 p. a ja direktiivi art. 4. Samas direktiivi pp. 26 viitab samuti läbipaistvale andmetöötlusele.
[65] Teave, mis tuleb anda, kui andmed koguti inimeselt endalt, on peaaegu kattuv teabega, mis tuleb anda, kui andmeid ei saadud inimeselt endalt (vrd. üldmääruse art. 13 ja 14). Seetõttu panime selle kokku üheks nimekirjaks, lisades asjakohasel juhul vastava rea ette klausli.

- vastutava töötleja nimi ja kontaktandmed;
- andmekaitsespetsialisti kontaktandmed (kui ta on määratud);
- kui andmed ei ole saadud inimeselt endalt – andmete liigid ning nende päritoluallikad;
- isikuandmete töötlemise eesmärk ning õiguslik alus (nt leping, nõusolek), sh
    - kui isikuandmeid töödeldakse vastutava töötleja või kolmanda isiku õigustatud huvi alusel, siis teave selle kohta (õigustatud huvi eeldab põhjendamist);
    - kui andmed küsitakse inimeselt endalt – teave selle kohta, mis andmete esitamine tuleneb õigusaktist või lepingust, samuti esitamata jätmise võimalikud tagajärjed (inimene peab saama aru, mis on kohustuslik, mis soovitatav ja mis selgelt vabatahtlik, ilma kahjulike tagajärgedeta);
    - kui andmed saadakse nõusoleku alusel, siis teave õiguse kohta nõusolek igal ajal tagasi võtta;
- isikuandmete säilitamistähtaeg või kui see ei ole võimalik, siis vähemalt tähtaja määramise põhimõtted;
- teave inimese õiguste kohta oma andmete osas:
    - õigus tutvuda oma andmetega,
    - asjakohasel juhul õigus nõuda andmete parandamist, kustutamist, töötlemise piiramist, andmete ülekandmist, samuti õigus esitada vastuväiteid,
    - õigus kaevata andmekaitseasutusele;
- kui andmeid edastatakse teistele isikutele - isikuandmete vastuvõtjad kas nimeliselt või vähemalt nende liigid;
- kui andmed kavatsetakse edastada kolmandasse riiki, siis täpsem asjakohane teave selle kohta;[66]
- kui tehakse automatiseeritud otsuseid – sellekohane teave, sh teave otsuste tegemise loogika ja otsuste mõju/tagajärgede kohta.

Kui andmeid kavatsetakse edasi töödelda muul eesmärgil, kui algselt koguti, siis tuleb teavitada muu eesmärgi ning muu asjakohase teabe osas enne töötlemise alustamist.

Kui eelnevat pikka nimekirja vaadata, siis on arusaadav, et tavalise asjaajamise käigus, kui sõlmitakse lepinguid või võetakse nõusolekuid või kus asutus teeb menetlusi, on kogu selle teabe igakordne esitamine tülikas. Seetõttu ongi mõistlik võtta eelnev kokku andmekaitsetingimusteks ning avaldada ettevõtte võrgulehel. Avaliku sektori asutustel on avaldamine seadusest tulenev kohustus.[67]

Andmekaitsetingimuste teavitamise vormi koostamise hõlbustamiseks oleme kokku pannud kontrollküsimustiku käesoleva juhise lisas 3.

Millal ei pea inimesele teavet andma?

Inimesele ei pea andma teavet selles osas, mis talle on juba niigi teada.

Kui inimene soovib teostada andmetega seotud õigusi (tutvuda, nõuda parandamist, kustutamist, piiramist, ülekandmist), siis nõuab andmetöötleja põhjendatud kahtluse korral isiku tuvastamist (digitaalse allkirjaga, isikut tõendada dokumendiga).

---

[66] Kolmandad riigid on kõik riigid ja rahvusvahelised organisatsioonid väljaspool Euroopa majanduspiirkonda. Euroopa majanduspiirkond on Euroopa Liit ning Island, Norra ja Liechtenstein.

[67] Avaliku teabe seaduse § 28 lg 1 p. 31^1 kohaselt tuleb teabevaldaja veebilehel avaldada: „isikuandmete töötlemise eesmärk, ulatus ja viis, kolmandatele isikutele, sealhulgas teisele asutusele, isikuandmete edastamise ja avalikkusele kättesaadavaks tegemise ning isiku poolt enda andmetega tutvumise õigus ja kord“.

Juhul, kui isikuandmeid ei ole kogutud inimeselt endalt, siis ei pea talle teada andma andmekaitsetingimustest:

a) kui andmete saamine või avaldamine on ette nähtud seaduses;

b) kui see nõuab ebaproportsionaalseid jõupingutusi (tingimusel, et on võetud kasutusele meetmed isiku huvide kaitseks, nt teave on avalikult kättesaadavaks tehtud) või

c) kui seadus nõuab andmete salajas hoidmist.

Üldmääruse art. 23 lubab liikmesriigi seadusandjal läbipaistvust täiendavalt kitsendada.

Vorm, tähtaeg, tasu

Andmekaitsetingimuste tekstile on sarnased nõuded nõusoleku tekstiga – see peab olema kokkuvõtlik, selge ja arusaadav ning lihtsasti kättesaadavas vormis.

Andmekaitsetingimustest teavitamise viise on mitmeid. Sobiva valiku peab andmetöötleja tegema ise lähtudes mõistlikkusest ning kasutajamugavusest. Teavet võib esitada nii suuliselt (kui isik seda nõuab), kirjalikult (nii eraldi dokumendina kui ka osana nõusoleku vormist) või elektrooniliselt (nt võrgulehel teavitusena või e-kirja teel). Heaks tavaks võib pidada seda, et andmekaitsetingimustest teavitatakse isikut samal viisil, mida kasutatakse andmete kogumiseks. Näiteks kogudes isikuandmeid elektroonilise vormi kaudu võiks seal samas ka isikule pakkuda selgitust andmete töötlemise kohta.

Elektrooniline andmekaitsetingimuste esitamine annab teavituseks ka enim viise ja võimalusi. Teavet võib esitada võrgulehel eraldi alalehena (viidates sellele andmeid saades), teavet võib esitada automaattekstina andmeid kogudes (nt isik täidab elektroonilist vormi, kus andmevälju täites ilmub automaatselt vastavasisuline teavitus), teavet võib esitada ühtse tekstina enne andmete andmist (nt nutiseadmetes kasutajatingimuste esitamine), teavet võib esitada video vahendusel jne.

Lisaks soovitame andmekaitsetingimuste esitamisel kasutada teksti liigendamist. Elektroonilisel esitamisel on võimalik alles vastavat (ala)pealkirja avades saada detailsem ülevaade. See võimaldab tekstist paremini aru saada ning endale olulist selekteerida. Samuti on teksti võimalik esitada ka vastavalt olukorrale erinevate nö kihtidena.

Olulisim andmekaitsetingimustest teavitamise puhul on siiski see, et teave oleks kergesti arusaadav ja lihtsasti kättesaadav. Eriti tuleb seda arvestada alaealistelt nõusoleku küsimisel ning ka nutiseadmete kasutamisel, kus teksti maht on ekraani väiksuse tõttu piiratud.

Andmekaitsetingimustest tuleb inimesele teatada temalt andmete kogumisel. Kui andmed ei ole saadud inimeselt endalt, tuleb reeglina teatada ühe kuu jooksul; kui neid kavatsetakse avaldada teistele isikutele, siis enne avaldamist.

Kui inimene soovib kasutada oma andmetega seotud õigusi (tutvumine, nõue parandada, kustutada, üle kanda, piirata), siis on tähtajaks üks kuu. Erandjuhul võib seda pikendada kahe kuu võrra (seega kokku kolm kuud). Pikendamisest ja selle põhjustest peab kuu jooksul taotlejale teada andma.

Tasu võib küsida üksnes juhul, kui taotlus on korduv, selgelt põhjendamatu või ülemäärane. Sellisel juhul võib küsida mõistlikku tasu arvestades tegelikke vajalikke kulutusi. Vastutaval töötlejal on kohustus tõendada taotluse põhjendamatust või ülemäärasust. Alternatiiv tasu küsimisele on taotluse rahuldamata jätmine, ka seda tuleb põhjendada.

Lisa 1. Andmekaitsealase mõjuhinnangu tegemise kontrollnimekiri

Isikuandmete kaitse üldmäärus näeb ette enne kõrge ohuga andmetöötlusega alustamist viia läbi andmekaitsealane mõjuhinnang. See on tegevus, mille käigus andmetöötleja hindab ja analüüsib, milliseid isikuandmeid ja milliste vahenditega ta oma tegevuse eesmärkide täitmiseks töötleb ning kas ja milliseid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid rakendab. Mõjuhinnang on oluline tööriist, mis annab organisatsiooniülese teadmise andmetöötlustoimingutest tervikuna. See võimaldab hinnata, kas andmete kaitseks rakendatavad asjakohased meetmed on piisavad, et üksikisikule tekkivat võimalikku kõrget privaatsusriivet leevendada vastuvõetavale tasemele.

Euroopa andmekaitseasutused on koostanud mõjuhinnnagu läbiviimise kontrollnimekirja, mille järgimine aitab tagada vastavust üldmäärusega.

Koostatakse isikuandmete töötlemise toimingute kirjeldus, mille käigus (art. 35 lg 7 p. a):

- ☐ arvestatakse töötlemise laadi, ulatust, konteksti ja eesmärke (pp. 90);
- ☐ registreeritakse töödeldavad isikuandmed, nende saajad ja andmete säilitustähtajad;
- ☐ kaardistatakse varad, kes või mis andmetöötluses osalevad (töötajad, riist- ja tarkvara, andmesideseadmed, andmekandjad);
- ☐ kui on olemas, arvestatakse valdkonna toimimisjuhenditega (art. 35 lg 8);

Hinnatakse isikuandmete töötlemise toimingute vajalikkust ja proportsionaalsust (art. 35 lg 7 p. b) ning kavandatakse meetmed isikuandmete kaitsele (art. 35 lg 7 p. d, pp. 90), võttes arvesse:

- ☐ isikuandmete kogumise täpselt ja selgelt kindlaksmääratud ning õiguspäraseid eesmärke (art. 5 lg 1 p. b);
- ☐ isikuandmete töötlemise seaduslikkust (art. 6);
- ☐ töödeldavate isikuandmete minimaalsust st töödeldakse ainult neid andmeid, mis on vajalikud eesmärkide täitmiseks (art. 5 lg 1 p. c);
- ☐ isikuandmete säilitustähtaegu st andmeid säilitatakse ainult seni, kuni see on vajalik eesmärkide täitmiseks (art. 5 lg1 p. e);
- ☐ isikuandmete töötlemise turvalisust (art. 32);
- ☐ isiku teavitamise kohustust (art. 12-14);
- ☐ isiku õigust tutvuda andmetega ning õigust andmete ülekandmisele (art. 15 ja 20);
- ☐ isiku õigust andmete parandamisele ja kustutamisele (art. 16, 17 ja 19);
- ☐ isiku õigust vastuväidete esitamiseks ning õigust isikuandmete töötlemise piiramisele (art. 18, 19 ja 21);
- ☐ suhteid volitatud töötlejatega (art. 28);
- ☐ kaitsemeetmeid isikuandmete edastamisel kolmandatele riikidele ja rahvusvahelistele organisatsioonidele (peatükk 5);
- ☐ järelevalveasutusega eelkonsulteerimist (art. 36).

Hinnatakse isikuandmete töötlemise toimingutega kaasnevaid võimalikke ohte (art. 35 lg 7 p. c), võttes arvesse:

- ☐ ohu päritolu, allikaid, laadi, eripära, tõenäosust ja mõju (pp. 84, 90) andmete käideldavusele, terviklusele ja konfidentsiaalsusele;
- ☐ ohu realiseerumisel isikule tekkivat võimalikku füüsilist, varalist või mittevaralist kahju (nt maine kahju, rahaline kahju, identiteedivargus või –pettus, diskrimineerimine (pp. 75)). Teisisõnu, määratakse isikule tekkiva tõenäolise ohu (kahju) tase;
- ☐ **Valitakse turvameetmed ohtude (riskide) haldamiseks ning aktsepteeritakse jääkrisk (art. 35 lg 7 p. d), pp. 90).**

Kaasatakse huvitatud isikud:

- ☐ küsitakse nõu andmekaitsespetsialistilt (art. 35 lg 2);
- ☐ vajaduse korral küsitakse isikute või nende esindajate seisukohti (art. 35 lg 9).

Lisa 2. Nõusoleku kontrollküsimustik

KOHUSTUS	OK √	KOMMENTAAR
Olen võimeline tõendama nõusoleku andmist	☐	Nõusolek on olemas suuliselt, kirjalikult või elektroonilises versioonis (nt isik on märgistanud vastava lahtri). NB! Vaikimist või tegevusetust ei peeta nõusoleku andmiseks!
Nõusoleku vormis EI OLE eelnevalt täidetud lahtreid	☐	Nõusoleku andmiseks peab isik täitma linnukesega lahtrid.
Nõusoleku vorm on konkreetne ning sõnastus on lihtsas keeles	☐	Nõusolek peab olema arusaadav, konkreetne, teadlik, ühemõtteline.
Nõusoleku küsimine on muudest küsimustest selgesti eristatud ning lihtsasti kättesaadav	☐	Kui nõusoleku taotlus käsitleb ka muid küsimusi, siis peab nõusoleku osa olema selgesti eristatav.
Isikul on nõusoleku andmiseks valikuvõimalus ning nõusolekust keeldumisel ei järgne talle kahjulikke tagajärgi	☐	Nõusolek peab olema vabatahtlikult antud.
Isik annab informeeritud nõusoleku	☐	Nõusoleku andmisel on isik informeeritud andmetöötlemise tingimustest ning tema õigustest
Isikul on õigus nõusolek tagasi võtta	☐	Nõusoleku tagasivõtmine ei mõjuta eelnevat nõusoleku alusel toimunud andmete töötlemist.
Olen kindlaks teinud alaealiselt nõusoleku küsimisel tema vanuse	☐	Infoühiskonna teenuste puhul saab isikuandmete töötlemiseks nõusoleku anda ka alaealine. Sellisel juhul on nõusoleku alampiiriks Eestis kehtestatud 13 aastat.
Nõusoleku vormis on teave andmete vastutava töötleja kohta	☐	Isik peab olema teadlik, kes on andmete vastutav töötleja ning millised on tema kontaktandmed.
Nõusoleku vormis on teave andmete töötlemise eesmärkide kohta	☐	Isik peab olema teadlik, milleks tema isikuandmeid töödeldakse.
Mitme erineva eesmärgi puhul on isikul võimalus anda iga eesmärgi kohta eraldi nõusolek	☐	Nõusolekut ei loeta vabatahtlikult antuks, kui isikul puudub iga erineva eesmärgi korral eraldi otsustusõigus.
Eriliigilised (delikaatsed) isikuandmed on nõusoleku vormis eraldi välja toodud	☐	Isik peab olema teadlik, milliseid eriliigilisi (delikaatseid) andmeid tema kohta töödeldakse.
Nõusoleku tagasivõtmise võimalus on märgitud nõusoleku vormi	☐	Nõusoleku tagasivõtmine peab olema sama lihtne kui nõusoleku andmine ning sellest tuleb isikut nõusoleku võtmisel informeerida.

Lisa 3. Andmekaitsetingimuste kontrollküsimustik

KOHUSTUS	OK ✓	KOMMENTAAR
Isikuandmete töötlemise tingimused on esitatud kirjalikult	☐	Teavet võib esitada kirjalikult või elektroonselt, nt võrgulehel. Isiku taotlusel võib teavet esitada suuliselt, kui isikusamasus on tuvastatud.
Teavituse sõnastus on kokkuvõtlik, selgelt arusaadavas keeles ning lihtsasti kättesaadavas vormis	☐	Vajadusel tuleks kasutada täiendavalt visualiseerimist ja teksti kihilist esitamist. Erinevatele sihtgruppidele suunatud tekst peab olema neile arusaadavas ja lihtsas sõnastuses.
Andmete vastutav töötleja aitab kaasa isiku teavitamisele ning tema õiguste kasutamisele	☐	Isiku õiguste kasutamise ning andmekaitsetingimustest teavitamise eest ei küsita tasu. Välja arvatud, kui isiku taotlus teabe saamiseks on selgelt põhjendamatu või ülemäärane, siis võib küsida mõistlikku tasu.
Isikut teavitatakse andmete töötlemisest muudel eesmärkidel	☐	Kui vastutav töötleja kavatseb isikuandmeid edasi töödelda muudel eesmärkidel, kui algselt neid koguti, tuleb isikule eelnevalt edastada teave kõnealuse teabe edasise töötlemise eesmärkide kohta ning samuti vajadusel ka üldmääruse artiklis 14 lõikes 2 olev teave. NB! Vajadusel uuendada nõusolekud.
Teave isikuandmete töötlemise tingimuste ja asjaolude kohta, mis tuleb isikule esitada andmete kogumise ajal: • vastutava töötleja andmed; • andmekaitsespetsialisti andmed; • töötlemise õiguslik alus ja eesmärk; • teave õigustatud huvi kohta; • isikuandmete vastuvõtjad; • andmete säilitamise ajavahemik; • edastamine kolmandasse riiki; • teave, kas andmete esitamine on õigusaktist või lepingust tulenev kohustus või lepingu sõlmimiseks vajalik nõue; • automatiseeritud otsused ja profiilianalüüs.	☐	Isikut ei tule teavitada juhul, kui isikul on nimetatud teave juba olemas.
Teave isikuandmete töötlemise tingimuste ja asjaolude kohta, mis tuleb isikule esitada juhul, kui isikuanded on saadud mujalt: • vastutava töötleja andmed; • andmekaitsespetsialisti andmed;	☐	Teave tuleb isikule esitada hiljemalt ühe kuu jooksul võttes arvesse konkreetse töötlemise asjaolusid, välja arvatud: a) isikul on see teave juba olemas;

• töötlemise õiguslik alus ja eesmärk; • isikuandmete liigid; • teave õigustatud huvi kohta; • isikuandmete vastuvõtjad; • andmete säilitamise ajavahemik; • edastamine kolmandasse riiki; • isikuandmete allikas; • automatiseeritud otsused ja profiilianalüüs.		b) teabe esitamine on võimatu või nõuab ebaproportsionaalseid pingutusi (nt teadusuuringute ja statistika puhul); c) isikuandmete saamine või avaldamine on sätestatud seadusega või; d) isikuandmed on kaetud saladuse hoidmise kohustusega.
Isiku teavitatakse tema õigustest nii andmete kogumise ajal kui ka olukorras, kus andmeid ei koguta isikult endalt	☐	Isikut tuleb teavitada tema järgnevatest õigustest: • õigus taotleda juurdepääsu tema kohta käivatele isikuandmetele; • õigus nõuda andmete parandamist; • õigus nõuda andmete kustutamist; • õigus piirata isikuandmete töötlemist; • õigus esitada vastuväiteid isikuandmete töötlemisele; • õigus nõuda isikuandmete ülekandmist; • õigus, et isiku kohta ei võetaks vastu otsust, mis põhineb automatiseeritud töötlusel; • õigus nõusoleku tagasivõtmisele; • õigus esitada kaebus andmekaitse järelevalveasutusele. NB! Kehtivad samad mitteteavitamise erandid, kui üldiste andmekaitsetingimustest teavitamiste osas!

Lisa 4. Andmetöötluse laad, ulatus, kontekst, eesmärk, korrapärasus, süstemaatilisus

Isikuandmete kaitse üldmäärus sisustab 26 mõistet (vt art. 4). Õiguskaitseasutuste andmekaitsedirektiiv selgitab 16 mõistet (vt art. 3).[68] Samas kasutavad nii üldmäärus kui direktiiv mitmeid õiguslikult sisustamata ning küllalt laia tõlgendamisruumi võimaldavaid termineid, millele otseseid selgitusi õigusaktis pole antud, kuid millest arusaamine on õigusnormide täitmiseks oluline. Nendeks on isikuandmete töötlemise **laad, ulatus, kontekst, eesmärk**.

Nimetatud terminid on üldmääruses ja direktiivis läbivalt andmetöötlejatele üheks kriteeriumiks, et:

(1) rakendada isikuandmete kaitseks asjakohaseid turvameetmeid;
(2) rakendada lõimitud ja vaikimisi andmekaitse põhimõtteid;
(2) täita andmetöötlustoimingute registreerimiskohustust;
(3) teostada andmekaitsealane mõjude hindamine;
(4) käsitleda isikuandmetega seotud rikkumisi;
(5) määrata andmekaitsespetsialist.

Järgnevalt püüamegi neid termineid kontrollküsimustiku abil paremini avada. Andmetöötleja saab neid kasutades ise oma andmetöötlust hinnata.

1. Isikuandmete töötlemise laad, hindamisel arvestada:

1.1. Kuidas vastutav töötleja isikuandmeid töötleb. Kas ise või kasutab ka volitatud töötlejaid;
1.2. Kas isikuandmeid edastada kolmandatele isikutele;
1.3. Kas isikuandmeid töödeldakse paberil või elektrooniliselt (automatiseeritud);
1.4. Kas lisaks isikuandmetele töödeldakse ka eriliigilisi isikuandmed;[69]
1.5. Kas töödeldakse laste või vanurite (haavatavamad inimrühmad) isikuandmeid;
1.6. Kas andmetöötluses kasutatakse uusi, kaasaegseid tehnoloogiaid;
1.7. Kas isikuandmeid töödeldakse eraldi või kombineeritult teiste andmetega;
1.8. Kas töödeldavad isikuandmed on pärit avalikest allikatest (nt isik on ise avaldanud);
1.9. Kas andmetöötlusega (nt profileerimine) luuakse uut isikustatud teavet;
1.10. Kas andmetöötlusega kaasneb isikutele õiguslikke tagajärgi;

2. Isikuandmete töötlemise ulatus, hindamisel arvestada:

2.1. Andmetöötluses osalevate isikute ja nende kategooriate (nt kliendid, patsiendid) arv;
2.2. Töödeldavate isikuandmete ja nende liikide ehk andmekoosseisude arv (arvestades nt eriliigiliste isikuandmete osakaalu nn „tavalistes" isikuandmetes);
2.3. Kui laialt on organisatsioon ja seda toetav tehniline keskkond isikuandmete töötlemisse kaasatud (arvestades kaasvastutavate ja -volitatud töötlejate arvu, kolmandatele isikutele edastamist, andmetöötluses kasutatavaid infovarasid);
2.4. Kas isikuandmete töötlemine on organisatsiooni põhitegevuse osa või toimub see pigem erandkorras (on juhtumipõhine);
2.5. Milline on andmetöötluse geograafiline ulatus (nt kas ainult riigisisene või toimub ka piiriülene andmetöötlus).

[68] Direktiiv võeti üle isikuandmete kaitse seaduse 4. peatükiga. Selle peatüki üks säte, § 13, määratleb, et selle peatüki tähenduses kasutatakse termineid üldmääruse art. 4 ning art 9 lõike 1 tähenduses. Samas paragrahvis määratletakse ka ära õiguskaitseasutuse mõiste.
[69] Vt eriliigiliste isikuandmete määratlust üldmäärus art 9.

Ulatuslikku andmetöötlust selgitame pikemalt juhendi andmekaitsespetsialisti ja andmekaitsealase mõjuhinnangu peatükkides 3 ja 5.

3. Isikuandmete töötlemise kontekst, hindamisel arvestada:

3.1. Isikuandmete töötlemise eesmärke ja õiguslikke aluseid;
3.2. Millised pooled on isikuandmete töötlemisse kaasatud (nt analüütikud, turundajad, logistikud, inkassoettevõtted);
3.3. Kas isikuandmete töötlemise on organisatsiooni põhitegevuse lahutamatu osa või kõrvaltegevus;
3.4. Isikute kategooriaid, kelle isikuandmeid töödeldakse (nt töötajad, lapsed, vanurid, patsiendid, kliendid). Ehk, kas isikuandmeid töödeldakse nt töö- või kliendisuhetes, õppeprotsessis, tervishoiuteenuse osutamiseks, sotsiaalkaitse valdkonnas, turundustegevuses sh veebireklaamide näitamiseks;
3.5. Isikuandmete säilitamistähtaegu;
3.6. Kas ja kellele isikuandmeid edastatakse;
3.7. Millist tehnoloogiat isikuandmete töötlemisel kasutatakse (nt pilvetehnoloogia, töötajate isiklikud seadmed, sise- või avalikud võrgud, kas võrguliikluse ja andmete kaitseks on kasutusel kaasaegsed krüptolahendused).
3.8. Eri andmekoosseisude alustel isikuandmete kokkuviimise lihtsus isikuga (nn linkimine).

4. Isikuandmete töötlemise eesmärk, hindamisel arvestada:

4.1. Kas isikuandmeid töödeldakse organisatsiooni ja töötajate vahelise lepingu täitmiseks sh võrgu- ja infoturbe tagamiseks ning infovaradele ja ruumidele ligipääsude korraldamiseks;
4.2. Kas isikuandmeid töödeldakse toodete/teenuste pakkumiseks k.a müügi- ja turundustegevuse edendamiseks ning klienditoe osutamiseks;
4.3. Kas isikuandmeid töödeldakse isiku pöördumiste, avalduste, taotluste menetlemiseks;
4.4. Kas isikuandmeid töödeldakse seadusejärgsete kohustuste täitmiseks (nt raamatupidamise korraldamine, töötasu- ja maksude, kandideerimiste, puhkuste, töövõime, haiguspäevade arvestus).

5. Isikuandmete korrapärane töötlemine, hindamisel arvestada:

5.1. Kas isikuandmete töötlemine toimub pidevalt või kindlate ajavahemike tagant kindla perioodi jooksul;
5.2. Kas isikuandmete töötlemine toimub kindlaksmääratud aegadel;
5.3. Kas isikuandmete töötlemine toimub pidevalt või perioodiliselt.[70]

6. Isikuandmete süstemaatiline töötlemine, hindamisel arvestada:

6.1. Kas isikuandmete töötlemine toimub mingi süsteemi alusel;
6.2. Kas isikuandmete töötlemine on eelnevalt korraldatud, organiseeritud või metoodiline;
6.3. Kas isikuandmete töötlemine toimub andmete kogumise üldkava raames;
6.4. Kas isikuandmete töötlemine toimub strateegia elluviimise raames.[71]

[70] Euroopa andmekaitsenõukogu „Suunised andmekaitseametnike kohta“.
[71] Euroopa andmekaitsenõukogu „Suunised andmekaitseametnike kohta“. Vt ka Euroopa andmekaitsenõukogu „Suuniseid, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679“.