WP243 LISA – KORDUMA KIPPUVAD KÜSIMUSED

Selle lisa eesmärk on vastata lihtsas ja hõlpsasti loetavas vormingus peamistele küsimustele, mis võivad organisatsioonidel tekkida seoses isikuandmete kaitse üldmäärusest tulenevate uute nõuetega andmekaitseametniku määramiseks.

Andmekaitseametniku määramine (artikkel 37)

1 Millised organisatsioonid on kohustatud määrama andmekaitseametniku? (Artikli 37 lõige 1)

Isikuandmete kaitse üldmääruses nõutakse andmekaitseametniku määramist kolmel konkreetsel juhul:

- kui töötleja on avaliku sektori asutus või organ (olenemata sellest, milliseid andmeid töödeldakse);
- kui vastutava töötleja või volitatud töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud, mis tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise, ning
- kui vastutava töötleja või volitatud töötleja põhitegevuse moodustab andmete eriliikide või süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine.

Juhime Teie tähelepanu sellele, et liidu või liikmesriigi õigusega võidakse andmekaitseametniku määramist nõuda ka muudes olukordades. Ka juhul, kui isikuandmete kaitse üldmäärusega andmekaitseametniku määramist tingimata ei nõuta, võivad organisatsioonid mõnikord otsustada, et andmekaitseametniku vabatahtlik nimetamine tuleb kasuks. Artikli 29 alusel asutatud andmekaitse töörühm (artikli 29 töörühm) julgustab neid vabatahtlikke samme tegema.

Lisateavet leiate suuniste punktist 2.1.

2 Mida tähendab mõiste „põhitegevus“? (Artikli 37 lõike 1 punktid b ja c)

Sõna „põhitegevus“ võib tõlgendada peamise tegevusena, mis on vajalik vastutava töötleja või volitatud töötleja eesmärkide saavutamiseks. See hõlmab ka sellist tegevust, mille puhul isikuandmete töötlemine moodustab lahutamatu osa vastutava töötleja või volitatud töötleja tegevusest. Näiteks tuleb terviseandmete, muu hulgas patsiendi tervisekaardi töötlemist käsitada haigla ühe põhitegevusena ja seetõttu peavad haiglad määrama andmekaitseametniku.

Teisalt teevad kõik organisatsioonid teatavaid toetavaid toiminguid, näiteks maksavad töötajatele tasu või osutavad tavapärast IT-tuge. Need on organisatsiooni põhitegevuseks või peamiseks tegevuseks vajalikud tugitoimingud. Ehkki need toimingud on vajalikud või olulised, peetakse neid üldjuhul kõrvaltoiminguteks, mitte põhitegevuseks.

Lisateavet leiate suuniste punktist 2.1.2.

3 Mida tähendab mõiste „ulatuslik“? (Artikli 37 lõike 1 punktid b ja c)

Isikuandmete kaitse üldmääruses ei ole määratletud, mida mõeldakse ulatusliku all. Artikli 29 töörühm soovitab, et eelkõige tuleks selle hindamisel, kas isikuandmete töötlemine on ulatuslik, kaaluda järgmisi asjaolusid:

- puudutatud andmesubjektide arv – kas konkreetse arvuna või osakaaluna asjaomasest

elanikkonnast;
- andmete maht ja/või erinevate töödeldavate andmeühikute kogus;
- andmete töötlemise kestus või püsivus;
- andmete töötlemise geograafiline ulatus.

Mõned näited andmete ulatuslikust töötlemisest:

- patsiendiandmete töötlemine haiglas tavapärase tegevuse raames;
- linna ühistranspordisüsteemi kasutavate inimeste sõiduandmete töötlemine (näiteks sõidukaartide jälitamise abil);
- rahvusvahelise kiirtoiduketi klientide geograafilise asukoha andmete töötlemine reaalajas statistilistel eesmärkidel, kui seda teeb sellisele tegevusele spetsialiseerunud volitatud töötleja;
- kliendiandmete töötlemine kindlustusühingus või pangas tavapärase äritegevuse raames;
- isikuandmete töötlemine, mida teeb otsingumootor käitumispõhise reklaami edastamiseks;
- sisu, liiklust või asukohta puudutavate andmete töötlemine, mida teevad telefoni- või internetiteenuse osutajad.

Mõned näited andmete mitteulatuslikust töötlemisest:

- patsiendiandmete töötlemine, mida teeb üksik arst;
- süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemine, mida teeb üksik advokaat.

Lisateavet leiate suuniste punktist 2.1.3.

4 Mida tähendab mõiste „regulaarne ja süstemaatiline järelevalve“? (Artikli 37 lõike 1 punkt b)

Andmesubjektide regulaarne ja süstemaatiline järelevalve ei ole isikuandmete kaitse üldmääruses määratletud, kuid see hõlmab selgelt igasugust internetis toimuvat jälgimist ja profiilianalüüsi koostamist, sealhulgas käitumispõhise reklaami edastamiseks. Jälgimise mõiste ei piirdu siiski veebikeskkonnaga.

Artikli 29 töörühm tõlgendab sõna „regulaarne“ ühes või järgmises tähenduses:

- toimub pidevalt või kindlate ajavahemike tagant kindla perioodi jooksul;
- kordub kindlaksmääratud aegadel;
- toimub pidevalt või perioodiliselt.

Artikli 29 töörühm tõlgendab sõna „süstemaatiline“ ühes või järgmises tähenduses:

- toimub mingi süsteemi alusel;
- eelnevalt korraldatud, organiseeritud või metoodiline;
- toimub andmete kogumise üldkava raames;
- toimub strateegia elluviimise raames.

Näited: sidevõrgu käitamine; sideteenuste osutamine; e-posti ümbersuunamine; profiilianalüüsi tegemine ja hindamine riskihindamise eesmärgil (nt krediidireitingu tegemiseks, kindlustuspreemia suuruse kindlaksmääramiseks, pettuse ennetamiseks ja rahapesu tuvastamiseks); asukoha jälitamine, näiteks mobiilirakenduste abil; kliendiprogrammid; käitumispõhine reklaam; heaolu, tervisliku

seisundi ja terviseandmete jälgimine kantavate seadmete abil; videovalve; ühendatud seadmed, nt nutimõõdikud, nutiautod, targa maja süsteemid jne.

Lisateavet leiate suuniste punktist 2.1.4.

5 Kas organisatsioonid võivad määrata mitme peale ühe andmekaitseametniku? Kui võivad, siis millistel tingimustel? (Artikli 37 lõiked 2 ja 3)

Isikuandmete kaitse üldmääruse kohaselt võib kontsern määrata ühe andmekaitseametniku, tingimusel et ta on „hõlpsasti kättesaadav kõikidest tegevuskohtadest“. Kättesaadavuse all mõeldakse andmekaitseametniku ülesandeid kontaktisikuna nii seoses andmesubjektide ja järelevalveasutusega kui ka organisatsiooni sees. Tagamaks ettevõttesisese või -välise andmekaitseametniku kättesaadavuse, tuleb veenduda, et tema kontaktandmed on kättesaadavad kooskõlas isikuandmete kaitse üldmäärusega. Andmekaitseametnikul peab olema võimalus suhelda tulemuslikult andmesubjektidega ja teha koostööd asjaomaste järelevalveasutustega. See tähendab, et nimetatud suhtlemine peab toimuma asjaomaste järelevalveasutuste ja andmesubjektide kasutatava(te)s keel(t)es. Andmekaitseametniku isiklik kättesaadavus (kas füüsiliselt samades ruumides, kus ka töötajad asuvad, telefonitsi või muude turvaliste sidevahendite abil) on oluline tagamaks, et andmesubjektidel on võimalik andmekaitseametnikuga ühendust saada.

Lisateavet leiate suuniste punktist 2.3.

6 Kas andmekaitseametnik on võimalik määrata ka ettevõtteväliselt? (Artikli 37 lõige 6)

Jah, on. Artikli 37 lõike 6 kohaselt võib andmekaitseametnik olla vastutava töötleja või volitatud töötleja koosseisuline töötaja (ettevõttesisene andmekaitseametnik) või „täita ülesandeid teenuslepingu alusel“. See tähendab, et andmekaitseametnik võib olla ettevõtteväline; sellisel juhul täidab ta oma ülesandeid üksikisiku või organisatsiooniga sõlmitud teenuslepingu alusel.

Kui andmekaitseametnik on ettevõtteväline, kohaldatakse talle kõiki artiklites 37–39 sätestatud nõudeid. Nagu suunistes öeldud, võib juhul, kui andmekaitseametnikuna tegutseb väline teenuseosutaja, tegeleda andmekaitseametniku ülesannetega selle teenuseosutaja heaks töötavatest inimestest koosnev meeskond, keda juhib kliendi peamiseks kontaktisikuks määratud ja kliendi eest vastutav inimene. Sellisel juhul on oluline, et iga andmekaitseametniku ülesandeid täitev ettevõttevälise organisatsiooni liige vastaks kõigile isikuandmete kaitse üldmääruses sätestatud asjaomastele nõuetele.

Õigusselguse ja hea organisatsiooni eesmärgil soovitatakse suunistes jagada teenuslepinguga selgelt ülesanded andmekaitseametniku meeskonnas ja määrata üks konkreetne isik kliendile peamiseks kontaktisikuks ja vastutajaks.

Lisateavet leiate suuniste punktidest 2.3, 2.4 ja 3.5.

7 Millised on andmekaitseametniku vajalikud kutseoskused? (Artikli 37 lõige 5)

Isikuandmete kaitse üldmäärus näeb ette, et „[a]ndmekaitseametniku määramisel lähtutakse tema kutseoskustest ja eelkõige ekspertteadmistest andmekaitsealase õiguse ja tava kohta ning suutlikkusest täita artiklis 39 osutatud ülesandeid“.

Erialaste teadmiste vajalik tase tuleks määrata kindlaks vastavalt tehtavatele andmetöötlustoimingutele ning töödeldavate isikuandmete kaitsmise nõuetele. Näiteks juhul, kui andmete töötlemine on eriti keeruline või kui see hõlmab suurt hulka delikaatseid isikuandmeid, võib andmekaitseametnik vajada suuremaid ekspertteadmisi ja suuremat toetust.

Vajalike oskuste ja teadmiste hulka kuuluvad näiteks:

- teadmised liikmesriigi ja Euroopa Liidu andmekaitsealastest õigusaktidest ning tavadest, sealhulgas põhjalikud teadmised isikuandmete kaitse üldmäärusest;
- arusaamine tehtavatest töötlemistoimingutest;
- arusaamine infotehnoloogiast ja andmeturbest;
- teadmised ärisektorist ja organisatsioonist;
- võime edendada organisatsioonis andmekaitsekultuuri.

Lisateavet leiate suuniste punktist 2.4.

Andmekaitseametniku ametiseisund (artikkel 38)

8 Millised vahendid tuleb andmekaitseametnikule anda, et ta saaks oma ülesandeid täita?

Isikuandmete kaitse üldmääruse artikli 38 lõikes 2 on sätestatud, et organisatsioon peab andmekaitseametnikku toetama, „andes talle [tema] ülesannete täitmiseks ja ekspertteadmiste taseme hoidmiseks vajalikud vahendid ning juurdepääsu isikuandmetele ja isikuandmete töötlemise toimingutele“.

Olenevalt isikuandmete töötlemise toimingutest ning organisatsiooni tegevusest ja suurusest tuleb andmekaitseametnikule anda järgmised ressursid:

- tippjuhtkonna aktiivne toetus andmekaitseametniku tööle;
- andmekaitseametnikule piisava aja andmine oma ülesannete täitmiseks;
- piisav toetus rahaliste vahendite, infrastruktuuri (ruumid, seadmed, varustus) ja personali näol vastavalt vajadusele;
- andmekaitseametniku määramisest ametlikult kõigile töötajatele teatamine;
- ligipääs organisatsiooni teistele üksustele, et andmekaitseametnik saaks neilt vajalikku toetust, sisendit ja teavet;
- pidevõpe.

Lisateavet leiate suuniste punktist 3.2.

9 Millised kaitsemeetmed võimaldavad andmekaitseametnikul täita oma ülesandeid sõltumatul viisil? (Artikli 38 lõige 3)

Selleks et andmekaitseametnik saaks tegutseda sõltumatul viisil, on kehtestatud mitu kaitsemeedet, mis on nimetatud põhjenduses 97:

- vastutavad töötlejad ega volitatud töötlejad ei tohi anda juhiseid andmekaitseametniku ülesannete täitmise kohta;
- vastutav töötleja ei tohi andmekaitseametnikku tema ülesannete täitmise eest ametist vabastada ega karistada;
- ei tohi olla huvide konflikti muude võimalike ülesannete ja kohustustega.

Lisateavet leiate suuniste punktidest 3.3–3.5.

10 Millised on andmekaitseametniku „muud ülesanded ja kohustused“, mis ei tohi kaasa tuua huvide konflikti? (Artikli 38 lõige 6)

Andmekaitseametnik ei saa organisatsioonis olla sellisel ametikohal, millest tulenevalt ta peab otsustama isikuandmete töötlemise eesmärkide ja vahendite üle. Kuna organisatsiooniline struktuur on igas organisatsioonis erinev, tuleb olukorda igal üksikjuhul eraldi kaaluda.

Rusikareegli kohaselt võib huvide konflikt tekkida selliste töökohtade puhul nagu kõrgema juhtimistaseme töötajad (tegevjuht, tootmisjuht, finantsjuht, meditsiinivaldkonna juht, turundusjuht, personalijuht või IT-juht), kuid ka muude, organisatsioonilises struktuuris madalamal asuvate töökohtade puhul, kui nendega kaasneb otsustamine isikuandmete töötlemise eesmärkide ja vahendite üle.

Lisateavet leiate suuniste punktist 3.5.

Andmekaitseametniku ülesanded (artikkel 39)

11 Mida hõlmab isikuandmete kaitse üldmääruses mõiste „järgimise jälgimine“? (Artikli 39 lõike 1 punkt b)

Üldmääruse järgimise jälgimise kohustuse raames võivad andmekaitseametnikud teha eelkõige järgmisi toiminguid:

- koguda teavet isikuandmete töötlemise toimingute kohta;
- analüüsida ja kontrollida isikuandmete töötlemise toimingute õiguspärasust ning
- teavitada vastutavat töötlejat või volitatud töötlejat ning anda neile nõu ja soovitusi.

Lisateavet leiate suuniste punktist 4.1.

12 Kas andmekaitseametnik vastutab isikuandmete kaitse üldmääruse järgimata jätmise eest isiklikult?

Ei vastuta. Andmekaitseametnikud ei vastuta isikuandmete kaitse üldmääruse järgimata jätmise eest isiklikult. Isikuandmete kaitse üldmääruses on selgelt väljendatud, et hoopis vastutav töötleja või volitatud töötleja peab tagama isikuandmete töötlemise kooskõlas määrusega ja suutma seda tõendada (artikli 24 lõige 1). Andmekaitsenõuete järgimise eest vastutab vastutav töötleja või volitatud töötleja.

13 Millised on andmekaitseametniku ülesanded seoses andmekaitsealase mõjuhinnangu (artikli 37 lõike 1 punkt c) ja isikuandmete töötlemise toimingute registreerimisega (artikkel 30)?

Andmekaitsealase mõjuhinnanguga seoses peaks vastutav töötleja või volitatud töötleja küsima andmekaitseametnikult nõu muu hulgas järgmistes küsimustes:

- kas teha andmekaitsealane mõjuhinnang või mitte;
- millist metoodikat andmekaitsealase mõjuhinnangu tegemisel kasutada;
- kas teha andmekaitsealane mõjuhinnang ise või tellida see väljast;
- milliseid kaitsemeetmeid (sh tehnilisi ja organisatsioonilisi meetmeid) võtta selleks, et maandada kõiki andmesubjektide õiguste ja huvidega seotud riske;
- kas andmekaitsealane mõjuhinnang on tehtud õigesti ja kas selle järeldused (kas jätkata andmete töötlemist või mitte ja milliseid kaitsemeetmeid võtta) vastavad isikuandmete kaitse üldmäärusele.

Lisateavet leiate suuniste punktist 4.2.

Isikuandmete töötlemise toimingute registreerimise puhul on vastutav töötleja või volitatud töötleja ja mitte andmekaitseametnik kohustatud registreerima isikuandmete töötlemise toimingud. Vastutaval töötlejal või volitatud töötlejal ei takista siiski miski andmast andmekaitseametnikule ülesannet registreerida isikuandmete töötlemise toimingud vastutava töötleja või volitatud töötleja vastutusel. Sellist registrit tuleb käsitada ühe vahendina, mis võimaldab andmekaitseametnikul täita oma ülesandeid, mille sisu on õigusaktide järgimise jälgimine ning vastutava töötleja või volitatud töötleja teavitamine ja nõustamine.

Lisateavet leiate suuniste punktist 4.4.