Suunised

Suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta

Versioon 3.0

4. juuni 2019

Vastu võetud

Versioonid

Versioon 3.0	4. juuni 2019	2. lisa lisamine (2. lisa versioon 2.0 võeti vastu 4. juunil 2019 pärast avalikku konsultatsiooni)
Versioon 2.1	9. aprill 2019	Suuniste paranduse vastuvõtmine (punkt 45)
Versioon 2.0	23. jaanuar 2019	Suuniste vastuvõtmine pärast avalikku konsultatsiooni – samal kuupäeval võeti vastu 2. lisa (versioon 1.0) avaliku konsultatsiooni korraldamiseks
Versioon 1.0	25. mai 2018	Suuniste vastuvõtmine pärast avalikku konsultatsiooni

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) (edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse EMP lepingut, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018, eriti selle XI lisa ja protokolli nr 37,

võttes arvesse oma 25. mail 2018 vastu võetud kodukorra artikleid 12 ja 22,

võttes arvesse, et isikuandmete kaitse üldmääruse artikli 70 lõikega 4 on ette nähtud avalik konsulteerimine, ja arvestades 30. maist 2018 kuni 12. juulini 2018 suuniste üle toimunud avaliku konsultatsiooni ning 15. veebruarist kuni 29. märtsini 2019 2. lisa üle toimunud avaliku konsultatsiooni tulemusi,

ON VASTU VÕTNUD JÄRGMISED SUUNISED:

1 SISSEJUHATUS

1. Isikuandmete kaitse üldmäärusega (määrus (EL) 2016/279) on Euroopas andmete kaitsmiseks ette nähtud ajakohastatud raamistik, mis tugineb vastutuskohustusele ja põhiõiguste järgimisele. Selle uue raamistiku seisukohast on väga tähtsad mitmesugused meetmed, mis hõlbustavad isikuandmete kaitse üldmääruse sätetest kinnipidamist. Need meetmed hõlmavad teatud asjaoludel kohaldatavaid kohustuslikke nõudeid (sh andmekaitseametniku määramine ja andmekaitsealase mõjuhinnangu tegemine) ning vabatahtlikke meetmeid, nagu toimimisjuhendid ja sertifitseerimismehhanismid.
2. Enne isikuandmete kaitse üldmääruse vastuvõtmist sedastas artikli 29 töörühm, et sertifitseerimisel võib olla andmete kaitsmisel kohaldatavas vastutusraamistikus oluline roll[1]. Selleks et sertifitseerimine tagaks usaldusväärsed tõendid andmekaitsenõuete täitmise kohta, peavad olema kehtestatud selged eeskirjad, milles on sätestatud sertifitseerimise nõuded[2]. Selliste eeskirjade väljatöötamise õiguslik alus on isikuandmete kaitse üldmääruse artikkel 42.
3. Isikuandmete kaitse üldmääruse artikli 42 lõikes 1 on sätestatud järgmist:

   „Liikmesriigid, järelevalveasutused, andmekaitsenõukogu ja komisjon julgustavad eelkõige liidu tasandil andmekaitse sertifitseerimise mehhanismide ning andmekaitsepitserite ja -märgiste kasutuselevõttu selle tõendamiseks, et vastutavate töötlejate ja volitatud töötlejate

[1] Artikli 29 töörühma 13. juuli 2010. aasta arvamus 3/2010 vastutuse põhimõtte kohta (WP 173), punktid 69–71.
[2] Artikli 29 töörühma arvamus 3/2010 vastutuse põhimõtte kohta (WP 173), punkt 69.

isikuandmete töötlemise toimingud vastavad käesolevale määrusele. Arvesse võetakse mikro-, väikeste ja keskmise suurusega ettevõtjate konkreetseid vajadusi.“

4. Sertifitseerimismehhanismide[3] kasutamisel võib suureneda läbipaistvus andmesubjektide jaoks, ent ka ettevõtjatevahelistes suhetes, näiteks vastutavate töötlejate ja volitatud töötlejate omavahelises suhtluses. Isikuandmete kaitse üldmääruse põhjenduses 100 on sätestatud, et sertifitseerimismehhanismide kehtestamine võib parandada läbipaistvust ja määruse järgimist ning võimaldab andmesubjektidel hinnata asjaomaste toodete ja teenuste andmekaitse taset[4].

5. Isikuandmete kaitse üldmääruses ei ole sätestatud vastutavate töötlejate ja volitatud töötlejate õigust sertifitseerimisele ega kohustust lasta end sertifitseerida. Nagu on sätestatud artikli 42 lõikes 3, on sertifitseerimine vabatahtlik protsess, mis aitab tõendada isikuandmete kaitse üldmääruse täitmist. Liikmesriike ja järelevalveasutusi kutsutakse üles soodustama sertifitseerimismehhanismide loomist ning nende ülesanne on ka otsustada sidusrühmade kaasamine sertifitseerimise protsessi ja elutsüklisse.

6. Peale selle on heakskiidetud sertifitseerimismehhanismide järgimine asjaolu, mida järelevalveasutused peavad raskendava või kergendava tegurina arvesse võtma trahvi määramise otsuse tegemisel ja trahvi summa kindlaksmääramisel (artikli 83 lõike 2 punkt j)[5].

1.1 Suuniste kohaldamisala

7. Käesolevate suuniste kohaldamisala on piiratud – tegemist ei ole isikuandmete kaitse üldmääruse kohase sertifitseerimise käsiraamatuga. Suuniste põhieesmärk on kindlaks teha üldised nõuded ja kriteeriumid, mis võivad olla asjakohased isikuandmete kaitse üldmääruse artiklite 42 ja 43 kohaselt kehtestatud mis tahes liiki sertifitseerimismehhanismi puhul. Selleks tehakse suunistes järgmist:

    - vaadeldakse sertifitseerimise kui vastutuse võtmist kinnitava vahendi kasutamise põhjendatust;
    - selgitatakse artiklites 42 ja 43 sisalduvate sertifitseerimissätete põhimõisteid;
    - selgitatakse, mida on võimalik artiklite 42 ja 43 alusel sertifitseerida ja mis on sertifitseerimise eesmärk, ning
    - hõlbustatakse selle tagamist, et sertifitseerimise tulemus on otstarbekas, üheselt mõistetav ning võimalikult hästi korratav ja võrreldav, olenemata sertifitseerijast.

8. Isikuandmete kaitse üldmäärus võimaldab liikmesriikidel ja järelevalveasutustel rakendada artikleid 42 ja 43 mitmel moel. Suunistes antakse nõu artiklite 42 ja 43 tõlgendamise ja rakendamise kohta ning nendega aidatakse liikmesriikidel, järelevalveasutustel ja riiklikel

[3] Käesolevates suunistes nimetatakse sertifitseerimismehhanisme ning andmekaitsepitsereid ja -märgiseid ühiselt „sertifitseerimismehhanismideks“ (vt punkt 1.3.2).
[4] Põhjenduses 100 on sätestatud, et „selleks et parandada läbipaistvust ja [---] määruse järgimist, tuleks soodustada sertifitseerimismehhanismide [---] kehtestamist, mis annavad andmesubjektidele võimaluse kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset“.
[5] Vt artikli 29 töörühma suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta (WP 253).

akrediteerimisasutustel võtta sertifitseerimismehhanismide rakendamiseks kooskõlas isikuandmete kaitse üldmäärusega kasutusele järjekindlam, ühtlustatud lähenemisviis.

9. Suunistes esitatud nõuanded on olulised

    - pädevatele järelevalveasutustele ja Euroopa Andmekaitsenõukogule (edaspidi „andmekaitsenõukogu“) sertifitseerimiskriteeriumide artikli 42 lõike 5, artikli 58 lõike 3 punkti f ja artikli 70 lõike 1 punkti o kohasel heakskiitmisel;
    - sertifitseerimisasutustele sertifitseerimiskriteeriumide koostamisel ja läbivaatamisel enne nende esitamist pädevale järelevalveasutusele artikli 42 lõike 5 kohaseks heakskiitmiseks;
    - andmekaitsenõukogule andmekaitsepitseri artikli 42 lõike 5 ja artikli 70 lõike 1 punkti o kohasel heakskiitmisel;
    - järelevalveasutustele oma sertifitseerimiskriteeriumide koostamisel;
    - Euroopa Komisjonile, kellel on õigus võtta vastu delegeeritud õigusakte, et määrata kindlaks nõuded, mida tuleb arvesse võtta artikli 43 lõikes 8 osutatud sertifitseerimismehhanismide puhul;
    - andmekaitsenõukogule artikli 70 lõike 1 punkti q ja artikli 43 lõike 8 kohaselt Euroopa Komisjonile sertifitseerimisnõuete kohta arvamuse esitamisel;
    - riiklikele akrediteerimisasutustele, kes peavad võtma sertifitseerimisasutuste akrediteerimisel kooskõlas standardiga EN-ISO/IEC 17065/2012 arvesse sertifitseerimiskriteeriume ja artiklis 43 osutatud lisanõudeid, ning
    - vastutavatele töötlejatele ja volitatud töötlejatele oma isikuandmete kaitse üldmääruse täitmise strateegia kindlaksmääramisel ja sertifitseerimise kui selle määruse täitmist tõendava vahendi kaalumisel.

10. Andmekaitsenõukogu avaldab eraldi suunised selle kohta, kuidas määrata kindlaks kriteeriumid, mille alusel heaks kiita sertifitseerimismehhanismid kui vahendid, mida kasutada andmete edastamisel kolmandatele riikidele või rahvusvahelistele organisatsioonidele kooskõlas artikli 42 lõikega 2.

1.2 Isikuandmete kaitse üldmääruse kohase sertifitseerimise eesmärk

11. Artikli 42 lõikes 1 on sätestatud, et sertifitseerimismehhanismid võetakse kasutusele „selle tõendamiseks, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud vastavad käesolevale määrusele“.

12. Isikuandmete kaitse üldmääruses on esitatud näiteid olukordadest, kus heakskiidetud sertifitseerimismehhanisme võib kasutada selle tõendamiseks, et vastutavad töötlejad ja volitatud töötlejad täidavad oma kohustusi, mis on seotud

    - artikli 24 lõigetes 1 ja 3, artiklis 25 ning artikli 32 lõigetes 1 ja 3 osutatud asjakohaste tehniliste ja korralduslike meetmete rakendamisega ja nende meetmete olemasolu tõendamisega;

- artikli 28 lõigetes 1 ja 4 osutatud piisava tagatise (vastavalt volitatud töötlejalt vastutavale töötlejale ja alamtöötlejalt volitatud töötlejale) tõendamisega kooskõlas artikli 28 lõikega 5.

13. Kuna sertifikaat iseenesest ei tõenda määruse täitmist, vaid on pigem üks vahend, mida saab kasutada vastavuse tõendamiseks, tuleks see anda läbipaistvalt. Vastavuse tõendamiseks on vaja tõendavaid dokumente, eelkõige kirjalikke aruandeid, milles on kirjeldatud seda, kuidas kriteeriumid on täietud, ning – juhul kui need algselt ei olnud täidetud – parandusi ja parandusmeetmeid ning nende asjakohasust, millega põhjendatakse sertifikaadi andmist ja allesjätmist. Selle raames tuleb anda ülevaade konkreetsetest sertifikaadi andmise, sertifikaadi kehtivuse pikendamise või sertifikaadi tagasivõtmise otsustest. Tuleks esitada kohaldatavatest kriteeriumidest tulenevad põhjused, argumendid ja tõendid ning sertifitseerimise käigus kogutud faktidel või tehtud eeldustel põhinevad järeldused ja otsused.

1.3 Põhimõisted

14. Käesolevas jaos analüüsitakse artiklites 42 ja 43 kasutatud põhimõisteid. Analüüs aitab neid mõisteid ja isikuandmete kaitse üldmääruse kohase sertifitseerimise ulatust paremini mõista.

1.3.1 Mõiste „sertifitseerimine“ tõlgendamine

15. Isikuandmete kaitse üldmääruses ei ole mõistet „sertifitseerimine“ määratletud. Rahvusvaheline Standardiorganisatsioon (ISO) on määratlenud sertifitseerimise kui sõltumatu asutuse kirjaliku kinnituse (sertifikaadi) andmise selle kohta, et toode, teenus või süsteem vastab konkreetsetele nõuetele. Sertifitseerimist tuntakse ka kui kolmanda isiku teostatavat vastavuse hindamist ja sertifitseerimisasutustele võidakse osutada ka kui vastavushindamisasutustele. Standardis EN-ISO/IEC 17000:2004 (Vastavushindamine. Sõnavara ja üldpõhimõtted), millele on osutatud standardis ISO 17065, on sertifitseerimine määratletud järgmiselt: „toodete, protsesside ja teenuste nõuetele vastavuse tõendamine [---] kolmanda isiku poolt“.

16. Atesteerimine on „etteantud nõuete täidetust tõendava tõendi väljastamine, mis põhineb ülevaatuse [---] tulemusel tehtud otsusel“ (ISO 17000:2004 punkt 5.2).

17. Isikuandmete kaitse üldmääruse artiklite 42 ja 43 kohasel sertifitseerimisel tähendab sertifitseerimine kolmanda isiku poolset atesteerimist, mis on seotud vastutavate töötlejate ja volitatud töötlejate teostatavate isikuandmete töötlemise toimingutega.

1.3.2 Sertifitseerimismehhanismid, pitserid ja märgised

18. Isikuandmete kaitse üldmääruses ei ole mõisteid „sertifitseerimismehhanismid“, „pitserid“ ja „märgised“ määratletud ning neid kasutatakse koos. Sertifikaat on kinnitus nõuetele vastavuse kohta. Pitserit või märgist võib kasutada sertifitseerimisprotsessi eduka lõpuleviimise tähistamiseks. Pitser või märgis tähendab tavaliselt logo või sümbolit, mille olemasolu (lisaks

sertifikaadile) osutab sellele, et sertifitseerimise objekt on läbinud sertifitseerimismenetluses sõltumatu hindamise ja vastab normdokumentides, näiteks eeskirjades, standardites või tehnilistes kirjeldustes sätestatud konkreetsetele nõuetele. Isikuandmete kaitse üldmääruse kohase sertifitseerimise puhul on need nõuded sätestatud lisanõuetes, mis täiendavad standardis EN-ISO/IEC 17065/2012 esitatud sertifitseerimisasutuste akrediteerimise eeskirju ja pädeva järelevalveasutuse või andmekaitsenõukogu heakskiidetud sertifitseerimiskriteeriume. Isikuandmete kaitse üldmääruse kohase sertifikaadi, pitseri või märgise saab välja anda vaid pärast seda, kui akrediteeritud sertifitseerimisasutus või pädev järelevalveasutus on teostanud tõendite sõltumatu hindamise ja on kinnitanud, et sertifitseerimiskriteeriumid on täidetud.

19. Järgmises tabelis on kirjeldatud üht tüüpilist sertifitseerimise protsessi.

Vastutav töötleja või volitatud töötleja esitab taotluse	Sertifitseerimisasutus teostab vormilise kontrolli	Hindamine Eelhindamine	Hindamine Sertifitseerimise objekti hindamine	Hindamine Tulemuste valideerimine	Pädeva järelevalveasutuse teavitamine	Sertifitseerimine	Järelevalve	Sertifikaadi kehtivuse pikendamine
Kas sertifitseerimise objekti kirjeldus on üheselt mõistetav ja täielik?	Kas sertifitseerimise objekti kirjelduse saab vastu võtta?	Millised on kohaldatavad kriteeriumid?	Kas sertifitseerimise objekt vastab nendele kriteeriumidele?	Kas sertifitseerimise objekti puhul on kindlaks tehtud kõik asjaomased kriteeriumid?	Kas on esitatud sertifikaadi andmise või tagasivõtmise põhjused?	Kas saab väljastada sertifikaadi?	Kas sertifitseerimise objekt vastab jätkuvalt kindlaksmääratud kriteeriumidele?	Kas isikuandmete töötlemine vastab endiselt sertifitseerimiskriteeriumidele?
Kas sertifitseerimise objektiks olevatele töötlemistoimingutele on võimalik võimaldada juurdepääs?	Kas kõik dokumendid on täielikud ja ajakohased?	Millised on kohaldatavad hindamismeetodid?	Kas sertifitseerimise objektiga seotud dokumendid on korrektsed?	Kas hindamine on piisavalt dokumenteeritud?		Kas aruanded on avaldamisvalmis?	Kas sertifikaati/pitserit/märgist kasutatakse õigesti?	Kas täiustamist vajavate küsimustega on tegeletud rahuldavalt?
Artikli 42 lõige 6	Artikli 43 lõige 4	Artikli 43 lõige 4	Artikli 42 lõige 5 ja artikli 43 lõige 4	Artikli 43 lõige 4	Artikli 43 lõige 1 ja artikli 43 lõige 5	Artikli 43 lõige 1 ja artikli 42 lõige 7	Artikli 42 lõige 7	Artikli 42 lõige 7

2 JÄRELEVALVEASUTUSE ROLL

20. Artikli 42 lõikes 5 on sätestatud, et sertifikaadi väljastab akrediteeritud sertifitseerimisasutus või pädev järelevalveasutus. Isikuandmete kaitse üldmäärusega ei ole tehtud sertifikaatide väljastamisest järelevalveasutuste kohustust. Määrus võimaldab hoopiski rakendada mitut erinevat mudelit. Näiteks võib järelevalveasutus otsustada kasutada üht või mitut järgmistest variantidest:

- väljastada sertifikaadi ise kooskõlas oma sertifitseerimissüsteemiga;
- väljastada sertifikaadi ise kooskõlas oma sertifitseerimissüsteemiga, kuid delegeerida hindamisprotsessi läbiviimise tervikuna või osaliselt kolmandatele isikutele;
- luua oma sertifitseerimissüsteemi ja usaldada sertifitseerimismenetluse läbiviimise sertifitseerimisasutusele, kes väljastab sertifikaadi, ning

- julgustada turgu välja töötama sertifitseerimismehhanisme.

21. Järelevalveasutus peab samuti mõtestama oma rolli liikmesriigi tasandil akrediteerimismehhanismide kohta tehtavate otsuste valguses – eelkõige seda, kas järelevalveasutusel endal on isikuandmete kaitse üldmääruse artikli 43 lõike 1 alusel õigus akrediteerida sertifitseerimisasutusi. Seega määrab iga järelevalveasutus kindlaks, millist lähenemisviisi rakendada, et taotleda isikuandmete kaitse üldmääruse kohase sertifitseerimise laia eesmärki. Selle kindlaksmääramisel ei võeta arvesse üksnes artiklites 57 ja 58 sätestatud ülesandeid ja volitusi, vaid ka sertifitseerimist kui tegurit, millega tuleb arvestada trahvide määramisel, ja üldisemalt kui määruse täitmise tõendamise vahendit.

2.1 Järelevalveasutus kui sertifitseerimisasutus

22. Kui järelevalveasutus otsustab teostada sertifitseerimise, peab ta hoolikalt hindama oma rolli seoses ülesannetega, mis on talle määratud isikuandmete kaitse üldmääruse alusel. Järelevalveasutuse roll nende ülesannete täitmisel peaks olema läbipaistev. Järelevalveasutus peab pöörama tähelepanu eelkõige uurimisvolituste ja jõustamisvolituste lahususele, et vältida võimalikke huvide konflikte.

23. Tegutsedes sertifitseerimisasutusena, peab järelevalveasutus tagama sertifitseerimismehhanismi nõuetekohase kasutuselevõtu ja töötama välja või vastu võtma sertifitseerimiskriteeriumid. Peale selle on igal sertifikaate väljastaval järelevalveasutusel ülesanne väljastatud sertifikaadid korrapäraselt läbi vaadata (artikli 57 lõike 1 punkt o) ja õigus sertifikaat tagasi võtta, kui sertifitseerimise nõuded ei ole enam täidetud (artikli 58 lõike 2 punkt h). Nende nõuete täitmiseks on kasulik kehtestada sertifitseerimismenetlus ja protsessi käsitlevad nõuded ning – välja arvatud juhul, kui on sätestatud teisiti (nt liikmesriigi õiguses) – sõlmida konkreetse sertifikaati taotleva organisatsiooniga sertifitseerimist käsitlev õiguslikult jõustatav kokkulepe. Tuleks kanda hoolt selle eest, et selles sertifitseerimiskokkuleppes nõutakse sertifikaadi taotlejalt vähemalt sertifitseerimiskriteeriumide täitmist ning et see hõlmab vajalikke kokkuleppeid hindamise teostamiseks, kriteeriumide täitmise jälgimiseks ja korrapäraseks läbivaatamiseks, sealhulgas juurdepääsu teabele ja/või ruumidele, dokumenteerimist, aruannete ja tulemuste avaldamist ning kaebuste uurimist. Lisaks oodatakse, et järelevalveasutus järgiks artikli 43 lõikes 2 loetletud nõuete kõrval nõudeid, mis on sätestatud sertifitseerimisasutuste akrediteerimist käsitlevates suunistes.

2.2 Järelevalveasutuse lisaülesanded seoses sertifitseerimisega

24. Liikmesriikides, kus hakkavad tegutsema sertifitseerimisasutused, on järelevalveasutusel olenemata tema tegevusest volitus ja ülesanne

    - hinnata sertifitseerimissüsteemi kriteeriumeid ja koostada otsuse eelnõu (artikli 42 lõige 5);

    - edastada otsuse eelnõu andmekaitsenõukogule, kui tal on kavas sertifitseerimiskriteeriumid heaks kiita (artikli 64 lõike 1 punkt c ja lõige 7), ning võtta andmekaitsenõukogu arvamust arvesse (artikli 64 lõike 1 punkt c ja artikli 70 lõike 1 punkt t);

- kiita heaks sertifitseerimiskriteeriumid (artikli 58 lõike 3 punkt f), enne kui saab toimuda akrediteerimine ja sertifitseerimine (artikli 42 lõige 5 ja artikli 43 lõike 2 punkt b);
- avaldada sertifitseerimiskriteeriumid (artikli 43 lõige 6);
- tegutseda pädeva asutusena ELi-üleste sertifitseerimissüsteemide rakendamisel, mille tulemuseks võib olla andmekaitsenõukogu heakskiidetud Euroopa andmekaitsepitser (artikli 42 lõige 5 ja artikli 70 lõike 1 punkt o), ning
- anda sertifitseerimisasutusele korraldus a) jätta sertifikaat väljastamata või b) sertifikaat tagasi võtta, kui sertifitseerimise nõuded (sertifitseerimise menetlus või kriteeriumid) ei ole enam täidetud (artikli 58 lõike 2 punkt h).

25. Isikuandmete kaitse üldmäärusega on antud järelevalveasutustele ülesanne sertifitseerimiskriteeriumid heaks kiita, mitte need välja töötada. Selleks et sertifitseerimiskriteeriumid artikli 42 lõike 5 alusel heaks kiita, peaks järelevalveasutusel olema selge arusaam sellest, mida isikuandmete kaitse üldmääruse täitmise tõendamisega seoses oodata, eelkõige tõendamise ulatusest ja sisust, ning samuti oma ülesandest jälgida määruse kohaldamist ja tagada selle kohaldamine. Lisas on esitatud suunised, et tagada kriteeriumide heakskiitmise eesmärgil toimuval hindamisel ühtlustatud lähenemisviisi rakendamine.

26. Artikli 43 lõikes 1 on sätestatud, et sertifitseerimisasutus peab enne sertifikaadi väljastamist või selle kehtivuse pikendamist teavitama oma järelevalveasutust, et see saaks kasutada oma parandusvolitusi vastavalt artikli 58 lõike 2 punktile h. Peale selle nõutakse artikli 43 lõikes 5, et sertifitseerimisasutus esitaks pädevale järelevalveasutusele taotletud sertifikaadi väljastamise või sertifikaadi tagasivõtmise põhjused. Ehkki isikuandmete kaitse üldmäärus võimaldab järelevalveasutusel kindlaks määrata, kuidas see teave saada, vastuvõetavaks tunnistada ja läbi vaadata ning kuidas sellega ümber käia (nt sertifitseerimisasutuste aruandluse jaoks võidakse kasutada tehnilisi lahendusi), võidakse kehtestada protsess ja kriteeriumid edukate sertifitseerimisprojektide kohta sertifitseerimisasutuselt artikli 43 lõike 1 alusel saadud teabe ja aruannete töötlemiseks. Sellele teabele tuginedes saab järelevalveasutus kasutada oma volitust anda sertifitseerimisasutusele korraldus võtta sertifikaat tagasi või jätta sertifikaat väljastamata (artikli 58 lõike 2 punkt h), jälgida isikuandmete kaitse üldmääruse kohaste sertifitseerimisnõuete ja -kriteeriumide kohaldamist ning tagada nende nõuete ja kriteeriumide kohaldamine (artikli 57 lõike 1 punkt a ja artikli 58 lõike 2 punkt h). See toetab ühtlustatud lähenemisviisi ja parandab eri sertifitseerimisasutuste tehtavate sertifitseerimistoimingute võrreldavust ning aitab tagada, et järelevalveasutustel on olemas teave organisatsiooni sertifitseerimisstaatuse kohta.

3 SERTIFITSEERIMISASUTUSE ROLL

27. Sertifitseerimisasutuse roll on väljastada, vaadata läbi, pikendada ja tagasi võtta sertifikaate (artikli 42 lõiked 5 ja 7), tuginedes sertifitseerimismehhanismile ja heakskiidetud

kriteeriumidele (artikli 43 lõige 1). Selleks peab sertifitseerimisasutus või sertifitseerimissüsteemi omanik kindlaks määrama ja kehtestama sertifitseerimiskriteeriumid ja menetlused, sealhulgas menetlused kriteeriumide täitmise jälgimiseks, kriteeriumide läbivaatamiseks, kaebuste käsitlemiseks ja sertifikaatide tagasivõtmiseks. Sertifitseerimiskriteeriumide läbivaatamine on osa akrediteerimisprotsessist, mille raames vaadeldakse eeskirju ja menetlusi, mille alusel sertifikaate, pitsereid või märgiseid väljastatakse (artikli 43 lõike 2 punkt c).

28. Sertifitseerimismehhanismi ja sertifitseerimiskriteeriumide olemasolu on vajalik sertifitseerimisasutuse akrediteerimiseks artikli 43 alusel. Sertifitseerimiskriteeriumide ulatus ja liik, mis mõjutavad sertifitseerimismenetlusi ja vastupidi, avaldavad sertifitseerimisasutuse tegevusele suurt mõju. Neis kriteeriumides võidakse nõuda konkreetsete hindamismeetodite kasutamist, näiteks kohapealsete kontrollide tegemist ja toimimisjuhendi läbivaatamist. Need menetlused on akrediteerimiseks kohustuslikud ja neid on selgitatud põhjalikumalt akrediteerimist käsitlevates suunistes.

29. Isikuandmete kaitse üldmääruse kohaselt peab sertifitseerimisasutus esitama järelevalveasutustele teavet, eriti konkreetsete sertifikaatide kohta, mis on vajalik, et jälgida sertifitseerimismehhanismi kohaldamist (artikli 42 lõige 7, artikli 43 lõige 5 ja artikli 58 lõike 2 punkt h).

4 SERTIFITSEERIMISKRITEERIUMIDE HEAKSKIITMINE

30. Sertifitseerimiskriteeriumid on iga sertifitseerimismehhanismi lahutamatu osa. Seetõttu nõutakse isikuandmete kaitse üldmääruses, et pädev järelevalveasutus kiidaks sertifitseerimismehhanismi sertifitseerimiskriteeriumid heaks (artikli 42 lõige 5 ja artikli 43 lõike 2 punkt b). Euroopa andmekaitsepitseri puhul kiidab sertifitseerimiskriteeriumid heaks andmekaitsenõukogu (artikli 42 lõige 5 ja artikli 70 lõike 1 punkt o). Mõlemat sertifitseerimiskriteeriumide heakskiitmist on selgitatud allpool.

31. Andmekaitsenõukogu tunnustab järgmisi sertifitseerimiskriteeriumide heakskiitmise eesmärke:

    - nõuetekohaselt kajastada määruses (EL) 2016/679 sätestatud nõudeid ja kriteeriume, mis on seotud füüsiliste isikute kaitsmisega isikuandmete töötlemisel, ning
    - aidata kaasa isikuandmete kaitse üldmääruse ühtsele kohaldamisele.

32. Heakskiit antakse juhul, kui sertifitseerimiskriteeriumides kajastub täielikult isikuandmete kaitse üldmääruse nõue, mille kohaselt sertifitseerimismehhanism peab võimaldama vastutavatel töötlejatel ja volitatud töötlejatel tõendada määruse täitmist.

4.1 Pädeva järelevalveasutuse poolne kriteeriumide heakskiitmine

33. Pädev järelevalveasutus peab sertifitseerimiskriteeriumid heaks kiitma enne sertifitseerimisasutuse akrediteerimist või selle ajal. Heakskiit tuleb saada ka sama sertifitseerimisasutuse standardi ISO 17065 kohastele ajakohastatud või täiendavatele süsteemidele või kriteeriumidele, enne kui muudetud sertifitseerimismehhanisme hakatakse

kasutama (artikli 42 lõige 5 ja artikli 43 lõike 2 punkt b). Järelevalveasutused käsitlevad kõiki sertifitseerimiskriteeriumide heakskiitmise taotlusi õiglasel ja mittediskrimineerival viisil, kohaldades avalikkusele kättesaadavat menetlust, milles on kindlaks määratud täidetavad üldised tingimused ja kirjeldatud heakskiitmise protsessi.

34. Sertifitseerimisasutus saab väljastada sertifikaadi vaid konkreetses liikmesriigis koosõlas asjaomase liikmesriigi järelevalveasutuse heakskiidetud kriteeriumidega. Teisisõnu peab sertifitseerimiskriteeriumid heaks kiitma selle liikmesriigi pädev järelevalveasutus, kus sertifitseerimisasutus kavatseb sertifikaate väljastada ja kus sertifitseerimisasutus akrediteeritakse. Euroopa-üleseid sertifitseerimiskavu on käsitletud allpool.

4.2 Andmekaitsenõukogupoolne kriteeriumide heakskiitmine Euroopa andmekaitsepitseri jaoks

35. Sertifitseerimisasutus võib väljastada sertifikaate ka kooskõlas kriteeriumidega, mille andmekaitsenõukogu on heaks kiitnud Euroopa andmekaitsepitseri jaoks. Kui andmekaitsenõukogu kiidab sertifitseerimiskriteeriumid artikli 63 kohaselt heaks, võib tulemuseks olla Euroopa andmekaitsepitser (artikli 42 lõige 5). Olemasolevate sertifitseerimis- ja akrediteerimistavade valguses tunnistab andmekaitsenõukogu, et on soovitatav vältida andmekaitse sertifitseerimise turu killustamist. Andmekaitsenõukogu märgib, et artikli 42 lõike 1 kohaselt peavad liikmesriigid, järelevalveasutused, andmekaitsenõukogu ja komisjon julgustama eelkõige liidu tasandil sertifitseerimismehhanismide kasutuselevõttu.

4.2.1 Heakskiidu taotlemine

36. Taotlus saada kriteeriumidele artikli 42 lõike 5 ja artikli 70 lõike 1 punkti o kohaselt andmekaitsenõukogu heakskiit tuleb esitada pädeva järelevalveasutuse kaudu. Selles tuleb välja tuua süsteemi omaniku, akrediteerimist taotleva sertifitseerimisasutuse või akrediteeritud sertifitseerimisasutuse kavatsus kasutada asjaomaseid kriteeriumeid sertifitseerimismehhanismis, mida kohaldatakse kõikide liikmesriikide vastutavate töötlejate ja volitatud töötlejate suhtes. Pädev järelevalveasutus esitab andmekaitsenõukogule eelnõu, kui ta leiab, et andmekaitsenõukogu võiks kriteeriumid heaks kiita.

37. Otsus selle kohta, kas kriteeriumide heakskiitmise taotlus esitada, tehakse sertifitseerimissüsteemi omaniku või sertifitseerimisasutuse peakorteris.

38. Kui sertifitseerimisasutus esitab taotluse, teeb ta seda tavaliselt akrediteerimise taotlemisel või on ta oma liikmesriigi pädeva järelevalveasutuse või riikliku akrediteerimisasutuse poolt juba akrediteeritud. See, kui sertifitseerimisasutus on isikuandmete kaitse üldmääruse kohase sertifitseerimismehhanismi rakendamiseks juba akrediteeritud, võib aidata lihtsustada heakskiitmise protsessi.

4.2.2 Euroopa andmekaitsepitseri kriteeriumid

39. Andmekaitsenõukogu koordineerib hindamisprotsessi ja kiidab nõuetekohaselt heaks Euroopa andmekaitsepitseri kriteeriumid. Hindamisel vaadeldakse kriteeriumide ulatust ja suutlikkust tagada ühtne sertifitseerimine. Kui andmekaitsenõukogu kiidab kriteeriumid heaks, käsitleb sertifitseerimismehhanismiga seotud kaebusi sertifitseerimisasutuse ELi peakorteri pädev järelevalveasutus, kes teavitab neist ka teisi järelevalveasutusi. See järelevalveasutus on ka pädev võtma sertifitseerimisasutuse suhtes meetmeid. Vajaduse korral teavitab pädev järelevalveasutus teisi järelevalveasutusi ja andmekaitsenõukogu.

40. Ühtse sertifitseerimisega seotud kriteeriumid sõltuvad ELi-ülestest vajadustest ja nendega tuleks tagada konkreetne mehhanism nende vajaduste rahuldamiseks. Euroopa sertifitseerimismehhanismid peavad olema mõeldud kasutamiseks kõikides liikmesriikides. Artikli 42 lõike 5 alusel peavad Euroopa andmekaitsepitseri jaoks kasutatav mehhanism ja selle kriteeriumid olema kohandatavad, et võtta vajaduse korral arvesse liikmesriikide valdkondlikke õigusakte, nt andmete töötlemisel koolides, samuti tuleks kavandada nende kohaldamine kogu Euroopas.

41. Näide: liikmesriigis A asub rahvusvaheline kool, kus õpetatakse liidus elavaid andmesubjekte. Kool soovib sertifitseerida oma veebipõhise taotlemisprotsessi, kasutades ELi-ülest sertifitseerimissüsteemi, et saada Euroopa andmekaitsepitser. Kooli eesmärk on taotleda liikmesriigis B asuva sertifitseerimisasutuse töötlemistoimingute sertifitseerimist Euroopa andmekaitsepitseri abil. Kohaldades pitseriga seotud kriteeriumeid, mis on kavandatud ja dokumenteeritud asjaomases mehhanismis, peab olema võimalik arvesse võtta liikmesriigis A koolide suhtes kohaldatavaid õigusakte. Samuti tuleks kriteeriumides nõuda, et kooli veebipõhises taotlemisprotsessis esitataks teavet kohaldatavate liikmesriigi andmekaitsenõuete kohta, mis võivad olla teistes liikmesriikides teistsugused, ja võetaks neid nõudeid arvesse. Selline teave võib hõlmata taotlemisel esitatavaid isikuandmeid, nt eelkoolis saadud hindeid või tehtud testide tulemusi, erinevaid andmete säilitamise perioode, finants- või biomeetriliste andmete kogumist või töötlemist ja edasise töötlemise piiranguid.

    - Euroopa andmekaitsepitseri mehhanismi heakskiitmise kõrgetasemeliste kriteeriumide hulka kuuluvad
        - andmekaitsenõukogu heakskiidetud kriteeriumid;
        - kohaldamine eri jurisdiktsioonides, võttes vajaduse korral arvesse liikmesriikide õigusnõudeid ja valdkondlikke õigusakte;

    - ühtlustatud kriteeriumid, mis on kohandatavad, et kajastada liikmesriikide nõudeid;
        - sertifitseerimismehhanismi kirjeldus;
        - sertifitseerimiskokkulepped, milles tunnustatakse Euroopa-üleseid nõudeid;
        - menetlused, millega tagada lahendused riiklike erinevuste jaoks ja kanda hoolt selle eest, et pitser aitab tõendada isikuandmete kaitse üldmääruse täitmist, ning
        - kõigile asjassepuutuvatele järelevalveasutustele mõeldud aruannetes kasutatav keel.

42. Nõuandeid Euroopa andmekaitsepitseri kriteeriumide kohta on esitatud ka lisas.

4.2.3 Akrediteerimise roll

43. Nagu on märgitud punktis 4.2.1, kui kriteeriumid on tunnistatud ühtseks sertifitseerimiseks sobivaks ja andmekaitsenõukogu on need artikli 42 lõike 5 kohaselt heaks kiitnud, võidakse sertifitseerimisasutus akrediteerida teostama nende kriteeriumide alusel liidu tasandil sertifitseerimist.

44. Sertifitseerimissüsteemid, mis on mõeldud rakendamiseks vaid konkreetsetes liikmesriikides, ei saa taotleda ELi pitserit. Akrediteerimine Euroopa andmekaitsepitseri väljastamise volituse saamiseks peab toimuma liikmesriigis, kus asub süsteemi rakendama hakkava sertifitseerimisasutuse peakorter, mis vastutab sertifikaatide andmise ning oma teistes liikmesriikides asuvate üksuste ja tütarettevõtjate sertifitseerimistegevuse haldamise eest. Kui muud asutused või ametid haldavad ja teostavad sertifitseerimist iseseisvalt, peab igaüks neist olema oma asukohaliikmesriigis eraldi akrediteeritud. Teisisõnu piisab akrediteerimisest liikmesriigis, kus asub sertifitseerimisasutuse peakorter, vaid siis, kui sertifikaate väljastab üksnes peakorter. Kui sertifikaate väljastavad ka muud sertifitseerimisasutusele alluvad asutused, vajavad akrediteerimist ka need asutused.

45. Seega, kui sertifitseerimisasutust ei ole Euroopa andmekaitsepitseriga seotud sertifitseerimiseks akrediteeritud, ei ole võimalik andmekaitsenõukogu heakskiidetud kriteeriume kasutada ja pitserit väljastada.

5 SERTIFITSEERIMISKRITEERIUMIDE VÄLJATÖÖTAMINE

46. Isikuandmete kaitse üldmäärusega on kehtestatud raamistik sertifitseerimiskriteeriumide väljatöötamiseks. Ehkki sertifitseerimismenetluse põhinõudeid on käsitletud artiklites 42 ja 43, milles on sätestatud ka sertifitseerimismenetluse olulised kriteeriumid, tuleb sertifitseerimiskriteeriumide alus tuletada isikuandmete kaitse üldmääruse põhimõtetest ja eeskirjadest, mis aitavad ka tõendada, et kõnealused kriteeriumid on täidetud.

47. Sertifitseerimiskriteeriumide väljatöötamisel tuleks keskenduda kriteeriumide kontrollitavusele, olulisusele ja sobivusele määruse täitmise tõendamisel. Sertifitseerimiskriteeriumid tuleks sõnastada nii, et nad oleksid selged ja arusaadavad ning et neid oleks võimalik praktikas kohaldada.

48. Sertifitseerimiskriteeriumide koostamisel tuleks vajaduse korral arvesse võtta muu hulgas järgmisi töötlemistoimingu hindamist toetavaid vastavusaspekte:

    - isikuandmete töötlemise seaduslikkus vastavalt artiklile 6;
    - isikuandmete töötlemise põhimõtted vastavalt artiklile 5;
    - andmesubjektide õigused vastavalt artiklitele 12–23;
    - kohustus teavitada isikuandmetega seotud rikkumistest vastavalt artiklile 33;

- lõimitud andmekaitse ja vaikimisi andmekaitse kohustus vastavalt artiklile 25;
- kas on tehtud artikli 35 lõike 7 punkti d kohane andmekaitsealane mõjuhinnang (vajaduse korral) ning
- artikli 32 kohaselt kehtestatud tehnilised ja korralduslikud meetmed.

49. Need kaalutlused võivad kajastuda kriteeriumides erineval määral sõltuvalt sertifitseerimise ulatusest, mis võib piirduda teatud liiki töötlemistoimingu(te)ga või sertifitseerimise valdkonnaga (nt tervishoiusektor).

5.1 Mida saab isikuandmete kaitse üldmääruse alusel sertifitseerida?

50. Andmekaitsenõukogu leiab, et isikuandmete kaitse üldmäärus võimaldab sertifitseerida määruse alusel väga erinevaid objekte, seni kuni eesmärk on aidata tõendada, et vastutavate töötlejate ja volitatud töötlejate isikuandmete töötlemise toimingud on määrusega kooskõlas (artikli 42 lõige 1).

51. Töötlemistoimingu hindamisel tuleb vajaduse korral arvesse võtta järgmist kolme põhikomponenti:

    1. isikuandmed (isikuandmete kaitse üldmääruse sisuline kohaldamisala);
    2. tehnilised süsteemid – isikuandmete töötlemiseks kasutatav taristu, nt riist- ja tarkvara, ning
    3. töötlemistoimingu(te)ga seotud protsessid ja menetlused.

52. Igat töötlemistoimingu komponenti tuleb hinnata kindlaksmääratud kriteeriumide alusel. Mõju võivad avaldada vähemalt neli olulist tegurit: 1) vastutava töötleja või volitatud töötleja organisatsiooniline ja õiguslik struktuur; 2) töötlemistoimingu(te)ga seotud osakond, keskkond ja inimesed; 3) hinnatavate elementide tehniline kirjeldus ning 4) töötlemistoimingut toetav IT-taristu, sealhulgas operatsioonisüsteemid, virtuaalsüsteemid, andmebaasid, autentimis- ja loasüsteemid, ruuterid ja tulemüürid, hoiusüsteemid, sidetaristu või internetiühendus ning seonduvad tehnilised meetmed.

53. Kõik kolm põhikomponenti on olulised sertifitseerimismenetluste ja -kriteeriumide kavandamisel. Neid võidakse arvesse võtta eri määral sõltuvalt sertifitseerimise objektist. Näiteks mõnel juhul võib mõne komponendi tähelepanuta jätta, kui leitakse, et see ei ole sertifitseerimise objekti puhul oluline.

54. Et veelgi täpsustada, mida saab isikuandmete kaitse üldmääruse alusel sertifitseerida, on määruses esitatud lisasuunised. Artikli 42 lõikest 7 tuleneb, et isikuandmete kaitse üldmääruse alusel väljastatakse sertifikaate üksnes vastutavatele töötlejatele ja volitatud töötlejatele, millega on välistatud näiteks andmekaitseametnike sertifitseerimine. Artikli 43 lõike 1 punktis b on osutatud standardile ISO 17065, millega on ette nähtud toodete, teenuste ja protsesside vastavust hindavate sertifitseerimisasutuste akrediteerimine. Töötlemistoimingu või mitme töötlemistoimingu tulemuseks võib olla kõnealuse standardi terminoloogia kohaselt toode või teenus ja selle suhtes võidakse kohaldada sertifitseerimist. Näiteks töötaja andmete

töötlemine palga maksmiseks või puhkuste haldamiseks koosneb reast töötlemistoimingutest isikuandmete kaitse üldmääruse tähenduses ning selle tulemuseks võib olla ISO terminoloogia kohaselt toode, protsess või teenus.

55. Nende kaalutluste põhjal leiab andmekaitsenõukogu, et isikuandmete kaitse üldmääruse kohane sertifitseerimine hõlmab eelkõige töötlemistoiminguid või töötlemistoimingute kogumeid. Need võivad sisaldada korralduslikes meetmetes väljenduvaid juhtimisprotsesse, mis moodustavad töötlemistoimingu lahutamatu osa (nt kaebuste käsitlemiseks sisse seatud juhtimisprotsess, mida rakendatakse töötaja andmete töötlemisel palga maksmise eesmärgil).

56. Selleks et hinnata töötlemistoimingu vastavust sertifitseerimiskriteeriumidele, peab olema esitatud konkreetne kasutusjuhtum. Näiteks töötlemistoimingu sooritamisel kasutatava tehnilise taristu kasutamise vastavus sõltub sellest, mis liiki andmeid sellega kavatsetakse töödelda. Korralduslikud meetmed sõltuvad andmete liigist ja kogusest ning töötlemisel kasutatavast tehnilisest taristust ning arvesse tuleb võtta töötlemise laadi, ulatust, sisu ja eesmärki ning andmesubjektide õigusi ja vabadusi ähvardavaid ohte.

57. Peale selle tuleb meeles pidada, et IT-rakendused võivad olla väga erinevad, isegi kui neid kasutatakse samal töötlemise eesmärgil. Seda tuleb arvesse võtta sertifitseerimismehhanismide ulatuse kindlaksmääramisel ja sertifitseerimiskriteeriumide koostamisel – sertifitseerimise ulatus ja kriteeriumid ei tohiks olla nii kitsad, et välistaksid erinevalt kavandatud IT-rakenduste kasutamise.

5.2 Sertifitseerimise objekti kindlaksmääramine

58. Sertifitseerimismehhanismiga seotud sertifitseerimisprojektide puhul tuleb eristada sertifitseerimismehhanismi kohaldamisala selle sertifitseerimise objektist, mida nimetatakse ka hindamise objektiks. Sertifitseerimismehhanismi kohaldamisala on võimalik määratleda kas üldiselt või seoses konkreetse töötlemistoimingu liigi või töötlemise valdkonnaga. Nii saab kindlaks määrata mehhanismi kohaldamisalasse kuuluvad sertifitseerimise objektid (nt digihoidlas sisalduvate isikuandmete turvaline säilitamine ja kaitsmine). Igal juhul saab usaldusväärne ja otstarbekas vastavuse hindamine toimuda vaid siis, kui sertifitseerimisprojekti objekti on täpselt kirjeldatud. Tuleb selgelt kirjeldada, milliseid töötlemistoiminguid sertifitseerimise objekt hõlmab, ning seejärel nimetada, milliseid põhikomponente (andmed, protsessid ja tehniline taristu) hinnatakse ja milliseid mitte. Seda tehes tuleb alati arvesse võtta ja kirjeldada ka seoseid teiste protsessidega. On selge, et see, mis ei ole teada, ei saa olla osa hindamisest ja seega ei saa seda ka sertifitseerida. Sertifitseerimise objekt peab igal juhul olema sertifitseerimisel või sertifitseerimisega edastatava sõnumi vaatenurgast otstarbekas ning see ei tohiks kasutajat, klienti ega tarbijat eksitada.

59. [Näide 1]

    Pank on töötanud välja veebisaidi, et pakkuda oma klientidele internetipanganduse teenust. See teenus võimaldab teha ülekandeid, osta aktsiaid, sõlmida püsikorraldusi ja hallata kontot. Pank soovib sertifitseerida üldistele kriteeriumidele tugineva üldise andmekaitse sertifitseerimise mehhanismi raames järgmise:

a) Turvaline sisselogimine

Turvaline sisselogimine on töötlemistoiming, mis on lõppkasutajale arusaadav ja andmekaitse vaatenurgast asjakohane, kuna see mängib olulist rolli asjassepuutuvate isikuandmete turvalisuse tagamisel. Seepärast on see töötlemistoiming turvaliseks sisselogimiseks vajalik ja võib seega kujutada endast otstarbekat hindamise objekti, kui sertifikaadil on selgelt märgitud, et sertifitseeritud on vaid sisselogimises seisnev töötlemistoiming.

b) Veebi eesserver

Ehkki veebi eesserver võib olla andmekaitse vaatenurgast asjakohane, ei ole see lõppkasutajale arusaadav ja seetõttu ei saa see olla otstarbekas hindamise objekt. Peale selle ei ole kasutaja jaoks selge, milliseid veebisaidi teenuseid ja seega milliseid töötlemistoiminguid sertifikaat hõlmab.

c) Internetipangandus

Veebi eesserver koos tagaserveriga tähendavad internetipanganduse teenuse raames tehtavaid töötlemistoimingud, mis võivad olla kasutaja vaatenurgast otstarbekad. Sel juhul peab hindamise objekt hõlmama mõlemat. Samas ei pea hindamise objekt hõlmama töötlemistoimingud, mis ei ole internetipanganduse teenuse osutamisega otseselt seotud – näiteks toiminguid, mille eesmärk on tõkestada rahapesu.

Internetipanganduse teenus, mida pank oma veebisaidi vahendusel pakub, võib hõlmata ka muid teenuseid, mille jaoks on vaja omakorda töötlemistoiminguid. Selliseks teenuseks võib olla näiteks kindlustustoote pakkumine. Kuna see lisateenus ei ole internetipanganduse teenuse osutamisega otseselt seotud, ei pea hindamise objekt seda hõlmama. Kui see lisateenus (kindlustus) jäetakse hindamise alt välja, on veebisaidil paiknevad teenuse liidesed osa hindamise objektist ja seepärast tuleb neid kirjeldada, et teenustel selgelt vahet teha. Selline kirjeldus on vajalik selleks, et teha kindlaks kahe teenuse vahelised võimalikud andmevood ja neid hinnata.

60. [Näide 2]

Pank pakub oma klientidele teenust, mis võimaldab klientidel koondada mitmest pangast eri kontode ja krediitkaartidega seotud teavet (kontode liitmine). Pank soovib lasta oma teenuse isikuandmete kaitse üldmääruse alusel sertifitseerida. Pädev järelevalveasutus on heaks kiitnud konkreetse kogumi sertifitseerimiskriteeriume, milles keskendutakse seda liiki tegevusele. Sertifitseerimismehhanism hõlmab vaid järgmisi vastavuse aspekte:

- kasutaja autentimine ja
- vastuvõetavad viisid koondatavate andmete hankimiseks teistest pankadest/teenustest.

Kuna selle sertifitseerimismehhanismi kohaldamisala kindlaksmääramisel on hindamise objekt juba määratletud, ei ole asjaomase kohaldamisala puhul hindamise objekti võimalik otstarbekalt kitsendada ja sertifitseerida vaid konkreetsed aspektid või üks töötlemistoiming. Selle stsenaariumi korral peab hindamise objekt vastama konkreetsele kohaldamisalale.

5.3 Hindamismeetodid ja -metoodika

61. Et teha vastavushindamine, mis aitab tõendada töötlemistoimingute nõuetele vastavust, on vaja kindlaks määrata hindamismeetodid ja -metoodika. On vahe, kas teave hindamise jaoks saadakse vaid dokumentidest (millest üksi ei piisa) või kogutakse aktiivselt kohapeal hindamise objektile otse või kaudselt ligi pääsedes. Teabe kogumise viis mõjutab sertifitseerimise kaalu ning seepärast tuleks see kindlaks määrata ja seda kirjeldada.

    Sertifikaatide väljastamise ja korrapärase läbivaatamise menetlus peaks sisaldama detailset teavet selle kohta, kuidas määrata kindlaks hindamise asjakohane tase (põhjalikkus ja üksikasjalikkus), et täita sertifitseerimiskriteeriumid, ning selles peaks olema

    - üksikasjalikult kirjeldatud kohaldatud hindamismeetodeid ja järeldusi, milleni jõuti näiteks kohapealsete auditite või dokumentide põhjal;
    - toodud välja hindamismeetodid, milles keskendutakse töötlemistoimingutele (andmed, süsteemid, protsessid) ja töötlemise eesmärgile;
    - määratud kindlaks andmete liigid ja kaitsevajadused ning selgitatud välja, kas töötlemisse on kaasatud volitatud töötlejad või kolmandad isikud;
    - määratud kindlaks rollid ning tehtud kindlaks rollide ja ülesannete põhjal määratletud juurdepääsukontrolli mehhanismi olemasolu.

62. Hindamise põhjalikkus mõjutab sertifitseerimise kaalukust ja väärtust. Vähendades hindamise põhjalikkust pragmaatilistel põhjustel või selleks, et kärpida kulusid, andmekaitse sertifitseerimise kaalukus kahaneb. Teisalt võivad hindamise üksikasjalikkust käsitlevad otsused ületada taotleja finantssuutlikkust ning sageli ka hindajate ja audiitorite suutlikkust. Vastavuse tõendamisel ei pruugi alati olla oluline analüüsida kasutatavaid IT-süsteeme väga üksikasjalikult, et analüüs oleks otstarbekas.

5.4 Hindamise dokumenteerimine

63. Sertifitseerimine tuleks põhjalikult dokumenteerida. Dokumentide puudumisel ei saa teha nõuetekohast hindamist. Sertifitseerimise dokumenteerimise olulisus seisneb selles, et sellega tagatakse sertifitseerimismehhanismi raames toimuva hindamise läbipaistvus. Dokumentidest leiab vastused seaduses sätestatud nõuetega seotud küsimustele. Sertifitseerimismehhanismides tuleks ette nähta standardne dokumenteerimismetoodika. Seejärel võimaldab hindamine võrrelda sertifitseerimisdokumente kohapeal valitseva tegeliku olukorraga ja sertifitseerimiskriteeriumidega.

64. Sertifitseerimise objekti ja kasutatud metoodika põhjalik dokumenteerimine tagab läbipaistvuse. Kooskõlas artikli 43 lõike 2 punktiga c peaksid sertifitseerimismehhanismides olema kindlaks määratud menetlused, mis võimaldavad sertifikaadid läbi vaadata. Üksikasjalikud dokumendid võivad olla kõige asjakohasem vahend, et võimaldada järelevalveasutustel hinnata, kas ja mil määral saab sertifitseerimist tunnustada ametlikes uurimistes. Seepärast tuleb hindamise dokumenteerimisel keskenduda kolmele põhiaspektile:

    - kasutatud hindamismeetodite järjepidevus ja sidusus;

- hindamismeetodid, mille abil tõendatakse sertifitseerimise objekti vastavust sertifitseerimiskriteeriumidele ja seega kooskõla määrusega, ning
- sõltumatu ja erapooletu sertifitseerimisasutusepoolne hindamistulemuste valideerimine.

5.5 Tulemuste dokumenteerimine

65. Põhjenduses 100 on esitatud teavet eesmärkide kohta, mida taotletakse sertifitseerimise sisseseadmisega:

„Selleks et parandada läbipaistvust ja käesoleva määruse järgimist, tuleks soodustada sertifitseerimismehhanismide, andmekaitsepitserite ja -märgiste kehtestamist, mis annavad andmesubjektidele võimaluse kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset.“

66. Dokumenteerimisel ja tulemuste edastamisel on läbipaistvuse parandamisel oluline roll. Sertifitseerimisasutused, kes kasutavad andmesubjektidele (kui tarbijatele või klientidele) suunatud sertifitseerimismehhanisme, pitsereid või märgiseid, peaksid andma sertifitseeritud töötlemistoimingu(te) kohta hõlpsasti kättesaadavat, arusaadavat ja sisulist teavet. See avalik teave peaks sisaldama vähemalt
    - hindamise objekti kirjeldust;
    - viidet konkreetse hindamise objekti suhtes kohaldatud heakskiidetud kriteeriumidele;
    - kriteeriumide hindamise metoodikat (kohapealne hindamine, dokumentide hindamine jne);
    - teavet sertifikaadi kehtivuse kestuse kohta ning
    - see peaks võimaldama järelevalveasutustel ja avalikkusel tulemusi võrrelda.

6 SERTIFITSEERIMISKRITEERIUMIDE KINDLAKSMÄÄRAMISE SUUNISED

67. Sertifitseerimiskriteeriumid on sertifitseerimismehhanismi lahutamatu osa. Sertifitseerimismenetlus sisaldab nõudeid konkreetset hindamise objekti käsitleva sertifitseerimisprojekti raames toimuva hindamise viisi, läbiviija, ulatuse ja üksikasjalikkuse kohta. Sertifitseerimiskriteeriumides sätestatakse nõuded, mille põhjal hinnatakse hindamise objektiks olevat tegelikku töötlemistoimingut. Käesolevates sertifitseerimiskriteeriumide kindlaksmääramise suunistes antakse üldist nõu, mis hõlbustab sertifitseerimiskriteeriumide hindamist nende heakskiitmise eesmärgil.
    - Sertifitseerimiskriteeriumide heakskiitmisel või kindlaksmääramisel tuleks arvesse võtta järgmisi üldisi kaalutlusi. Sertifitseerimiskriteeriumid peaksid olema

- ühtsed ja kontrollitavad;
- auditeeritavad, et hõlbustada töötlemistoimingute hindamist isikuandmete kaitse üldmääruse alusel, sisaldades eelkõige eesmärke ja rakendusjuhiseid nende eesmärkide saavutamiseks;
- sihtrühma seisukohast (nt ettevõtjalt ettevõtjale, ettevõtjalt kliendile) asjakohased;
- kooskõlas muude standarditega (nt ISO standardid, riiklikud standardid) ja vajaduse korral nendega koostalitlusvõimelised ning
- paindlikud ja kohandatavad kohaldamiseks eri liiki ja suurusega organisatsioonide puhul, sealhulgas mikro-, väikeste ja keskmise suurusega ettevõtjate puhul vastavalt artikli 42 lõikele 1, ja kooskõlas põhjenduse 77 kohase riskipõhise lähenemisviisiga.

68. Kohalik väikeettevõtja, näiteks jaemüüja, teostab tavaliselt vähem keerukaid isikuandmete töötlemise toiminguid kui suur rahvusvaheline jaemüüja. Ehkki töötlemistoimingute seaduslikkusega seotud nõuded on samad, tuleb arvesse võtta andmetöötluse ulatust ja keerukust. Seetõttu on vaja, et sertifitseerimismehhanismid ja nende kriteeriumid oleksid kohandatavad vastavalt asjaomasele töötlemistegevusele.

6.1 Olemasolevad standardid

69. Sertifitseerimisasutused peavad vaatlema, kuidas konkreetsetes kriteeriumides on arvesse võetud asjakohaseid olemasolevaid vahendeid, nagu toimimisjuhendid, tehnilised standardid või liikmesriikide regulatiivsed ja õiguslikud algatused. Ideaaljuhul on kriteeriumid koostalitlusvõimelised olemasolevate standarditega, mis võivad aidata vastutaval töötlejal või volitatud töötlejal täita oma isikuandmete kaitse üldmäärusest tulenevaid kohustusi. Ent kui tööstusharu standardites keskendutakse sageli organisatsiooni turvalisusele ja kaitsmisele ohtude eest, siis isikuandmete kaitse üldmääruse keskmes on füüsiliste isikute põhiõiguste kaitse. Seda teistsugust vaatenurka tuleb arvesse võtta, kui kavandatakse kriteeriume või kiidetakse heaks kriteeriume või sertifitseerimismehhanisme, mis põhinevad tööstusharu standarditel.

6.2 Kriteeriumide kindlaksmääramine

70. Sertifitseerimiskriteeriumid peavad vastama sertifitseerimismehhanismi või -süsteemiga edastatavale sõnumile ja ootustele, mida see tekitab. Sertifitseerimismehhanismi nimi võib juba sisaldada viidet mehhanismi kohaldamisalale ja mõjutab kriteeriumide kindlaksmääramist.

71. [Näide 3]

    Mehhanismi „terviseandmete privaatsuse märgis“ („HealthPrivacyMark“) kohaldamisala peaks piirduma tervishoiusektoriga. Pitseri nimi tekitab ootuse, et vaadeldud on terviseandmetega seotud andmekaitsenõudeid. Seega peavad selle mehhanismi kriteeriumid olema piisavad, et hinnata selle sektori andmekaitsenõudeid.

72. [Näide 4]

    Andmetöötluse juhtimissüsteeme hõlmavate töötlemistoimingute sertifitseerimisega seotud mehhanismi puhul tuleks kindlaks määrata kriteeriumid, mis võimaldavad tunnustada ja hinnata juhtimisprotsesse ning neid toetavaid tehnilisi ja korralduslikke meetmeid.

73. [Näide 5]

    Pilvandmetöötlusega seotud mehhanismi kriteeriumides tuleb arvesse võtta konkreetseid tehnilisi nõudeid, mis on vajalikud pilvepõhiste teenuste kasutamiseks. Näiteks, kui servereid kasutatakse väljaspool ELi, tuleb kriteeriumides arvestada tingimustega, mis on sätestatud isikuandmete kaitse üldmääruse V peatükis seoses andmete edastamisega kolmandatele riikidele.

74. Kriteeriumid, mis on kavandatud sobima eri hindamise objektidele eri sektorites ja/või liikmesriikides, peaksid sobima kohaldamiseks eri stsenaariumide korral; võimaldama kindlaks määrata väikeste, keskmiste või suurte töötlemistoimingute jaoks sobivad meetmed ning kajastama füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte kooskõlas isikuandmete kaitse üldmäärusega. Seega peavad kriteeriume täiendavad sertifitseerimismenetlused (nt dokumenteerimine, kontrollimine või hindamise meetod ja põhjalikkus) vastama nendele vajadustele ning võimaldama kehtestada või sisaldama eeskirju, näiteks asjakohaste kriteeriumide kohaldamiseks konkreetsete sertifitseerimisprojektide puhul. Kriteeriumid peavad hõlbustama selle hindamist, kas asjakohaste tehniliste ja korralduslike meetmete rakendamiseks on ette nähtud piisavad tagatised.

6.3 Sertifitseerimiskriteeriumide kasutusiga

75. Kuigi sertifitseerimiskriteeriumid peavad säilitama aja jooksul oma usaldusväärsuse, ei tuleks neid kivisse raiuda. Kriteeriumid peaks olema võimalik läbi vaadata, näiteks juhul kui

    - muudetakse õigusraamistikku;
    - tingimusi tõlgendatakse Euroopa Kohtu otsustes või
    - tehnika on edasi arenenud.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)

1. LISA. JÄRELEVALVEASUTUSTE ÜLESANDED JA VOLITUSED ISIKUANDMETE KAITSE ÜLDMÄÄRUSE KOHASEL SERTIFITSEERIMISEL

	Säte	Sisu
Ülesanded	Artikli 43 lõige 6	Järelevalveasutus peab avaldama kergesti kättesaadaval kujul artikli 42 lõikes 5 osutatud kriteeriumid ja edastama need andmekaitsenõukogule.
	Artikli 57 lõike 1 punkt n	Järelevalveasutus peab sertifitseerimiskriteeriumid artikli 42 lõike 5 kohaselt heaks kiitma.
	Artikli 57 lõike 1 punkt o	Järelevalveasutus vaatab vajaduse korral (st kui ta väljastab sertifikaate) korrapäraselt läbi artikli 42 lõike 7 kohaselt väljastatud sertifikaadid.
	Artikli 64 lõike 1 punkt c	Järelevalveasutus peab edastama andmekaitsenõukogule otsuse eelnõu, kui ta kavatseb kriteeriumid artikli 42 lõikes 5 osutatud sertifitseerimise eesmärgil heaks kiita.
Volitused	Artikli 58 lõike 1 punkt c	Järelevalveasutusel on volitus vaadata läbi artikli 42 lõike 7 kohaselt väljastatud sertifikaadid.
	Artikli 58 lõike 2 punkt h	Järelevalveasutusel on volitus võtta sertifikaat tagasi või anda sertifitseerimisasutusele korraldus võtta sertifikaat tagasi või jätta sertifikaat väljastamata.
	Artikli 58 lõike 3 punkt e	Järelevalveasutusel on volitus akrediteerida sertifitseerimisasutusi.
	Artikli 58 lõike 3 punkt f	Järelevalveasutusel on volitus väljastada sertifikaate ja kiita sertifitseerimiskriteeriumid heaks .

2. LISA

1 SISSEJUHATUS

2. lisas antakse suuniseid artikli 42 lõikes 5 sätestatud sertifitseerimiskriteeriumide läbivaatamiseks ja hindamiseks. Selles määratakse kindlaks küsimused, mida andmekaitse järelevalveasutus ja andmekaitsenõukogu võtavad arvesse ja kohaldavad, et sertifitseerimismehhanismi sertifitseerimiskriteeriumid heaks kiita. Nende küsimuste üle peaksid arutama sertifitseerimisasutused ja sertifitseerimissüsteemi omanikud, kes soovivad sertifitseerimiskriteeriume välja töötada ja heakskiitmiseks esitada. Nimekiri ei ole ammendav, vaid selles on loetletud küsimused, mida tingimata tuleb arvesse võtta. Kõik küsimused ei ole asjakohased, kuid neid tuleks kriteeriumide väljatöötamisel siiski arvesse võtta ning kui kriteeriumid ei hõlma teatavaid aspekte, tuleb seda vajaduse korral põhjendada. Mõned küsimused korduvad, sest need esitatakse eri perspektiivist. Suuniste järgimisel tuleks arvesse võtta isikuandmete kaitse üldmääruse ja vajaduse korral liikmesriikide õigusnõudeid.

2 SERTIFITSEERIMISMEHHANISMI KOHALDAMISALA JA HINDAMISE OBJEKT

a. Kas sertifitseerimismehhanismi (mille suhtes kasutatakse andmekaitse kriteeriume) kohaldamisala on selgelt kirjeldatud?

b. Kas sertifitseerimismehhanismi kohaldamisala on sihtgrupi seisukohast otstarbekas ega ole eksitav?

- *Näide. „Usaldusväärse äriühingu pitser“ („Trusted Company Seal“) viitab sellele, et terve äriühingu töötlemistoimingud on auditeeritud, isegi kui tegelikult tuleb sertifitseerida üksnes teatavad töötlemistoimingud, nt internetimaksed. Seetõttu on kohaldamisala eksitav.*

c. Kas sertifitseerimismehhanismi kohaldamisala võtab arvesse töötlemistoimingute kõiki aspekte?

- *Näide. „Terviseandmete privaatsuse märgis“ („HealthPrivacyMark“) peab hõlmama kõiki tervist käsitlevaid hindamisandmeid, et vastata artikli 9 kohastele nõuetele.*

d. Kas sertifitseerimismehhanismi kohaldamisala võimaldab isikuandmete kaitse otstarbekat sertifitseerimist, võttes arvesse asjaomaste töötlemistoimingutega seonduvate ohtude laadi ja sisu?

- *Näide. Kui sertifitseerimismehhanismi kohaldamisala on seotud üksnes töötlemistoimingute konkreetsete aspektidega, nagu andmete kogumine, aga mitte edasiste töötlemistoimingutega, nagu töötlemine reklaamiprofiili loomiseks või andmesubjekti õiguste haldamiseks, ei ole see andmesubjektide seisukohast otstarbekas.*

e. Kas sertifitseerimismehhanismi kohaldamisala hõlmab isikuandmete töötlemist asjaomases taotluse esitamise riigis või kas käsitletakse piiriülest andmete töötlemist ja/või edastamist?

f. Kas sertifitseerimiskriteeriumid kirjeldavad piisavalt seda, kuidas hindamise objekti tuleks määratleda?

- *Näide. „Privaatsusmärgis“ („Privacy Seal“), mille kohaldamisala on üldine ja eeldab üksnes nende töötlemistoimingute täpsustamist, mida tuleb sertifitseerida, ei anna piisavalt selgeid suuniseid, kuidas hindamise objekti kindlaks määrata ja kirjeldada.*
- *Näide. Andmete turvaliseks säilitamiseks kasutatava „digihoidla pitseri“ („The Privacy Vault Seal“) (konkreetne) kohaldamisala peaks kirjeldama üksikasjalikult nõudeid, millele kriteeriumid peavad vastama, et olla kohaldamisalaga kooskõlas, näiteks digihoidla määratlus, süsteemi nõuded ning kohustuslikud tehnilised ja korralduslikud meetmed. Sellisel juhul saab hindamise objekti määratleda kohaldamisala kaudu.*

    (1) Kas kriteeriumid eeldavad, et hindamise objekt hõlmab kõikide asjakohaste töötlemistoimingute kindlakstegemist, andmevoogude kirjeldamist ja hindamise objekti kohaldamisala kindlaksmääramist?

        - *Näide. Sertifitseerimismehhanism võimaldab sertifitseerida vastutavate töötlejate isikuandmete kaitse üldmääruse kohaseid töötlemistoiminguid, täpsustamata kohaldamise valdkonda (üldine kohaldamisala). Mehhanismis kasutatavad kriteeriumid eeldavad, et taotlev vastutav töötleja on määranud kindlaks asjaomase töötlemisoperatsiooniga seotud andmeliigid, süsteemid ja kasutatavad protsessid.*

    (2) Kas kriteeriumid eeldavad, et taotleja selgitaks, millal hinnatav töötlemine algab ja lõpeb? Kas kriteeriumid eeldavad, et hindamise objekti kindlaksmääramisel arvestatakse liideseid ka juhul, kui hindamise objekt ei sisalda omavahel seotud töötlemistoiminguid? Ja kas see on piisavalt põhjendatud?

        - *Näide. Hindamise objekt, mille puhul kirjeldatakse piisava üksikasjalikkusega selliste veebipõhiste teenuste töötlemistoiminguid nagu kasutajate registreerimine, teenuse osutamine, arveldamine, IP-aadresside logimine, liidesed kasutajatele ja kolmandatele isikutele, kuid ei käsitleta serverimajutust (aga käsitletakse töötlemist ning tehniliste ja korralduslike meetmetega seotud lepinguid).*

g. Kas kriteeriumid tagavad, et (konkreetsed) hindamise objektid on sihtrühmale, sealhulgas vajaduse korral andmesubjektidele, mõistetavad?

3 ÜLDNÕUDED

a. Kas kõik kriteeriumide komplektis (s.t kõik sertifitseerimiskriteeriumid) kasutatavad tingimused on kindlaks määratud, selgitatud ja kirjeldatud?

b. Kas kõik viited normidele on esitatud?

c. Kas kriteeriumid hõlmavad sertifitseerimismehhanismi kohaldamisalasse kuuluvate andmekaitsealaste vastutusvaldkondade, menetluste ja töötlemistoimingute määratlemist?

4 TÖÖTLEMISTOIMING, ARTIKLI 42 LÕIGE 1

Kas seoses sertifitseerimismehhanismi kohaldamisalaga (üldine või konkreetne) on kriteeriumide puhul kõiki töötlemistoimingute asjakohaseid komponente (andmed, süsteemid ja töötlemistoimingud) arvesse võetud?

a. Kas kriteeriumid eeldavad hindamise objekti kindlaksmääramisel töötlemistoimingu kehtiva õigusliku aluse täpsustamist?

b. Kas kriteeriumid võtavad hindamise objekti kindlaksmääramisel arvesse töötlemistoimingu asjaomaseid etappe ja andmete kogu elutsüklit, sealhulgas kustutamist ja anonüümimist?

c. Kas kriteeriumid eeldavad hindamise objekti kindlaksmääramisel andmete ülekantavust?

d. Kas kriteeriumid võimaldavad hindamise objekti kindlaksmääramisel arvestada konkreetset liiki töötlemistoiminguid, nt automatiseeritud otsuste tegemine ja profiilianalüüs?

e. Kas kriteeriumid võimaldavad hindamise objekti kindlaksmääramisel selgelt ära näidata konkreetsed andmete kategooriad?

f. Kas kriteeriumid võimaldavad ja eeldavad konkreetsete töötlemistoimingutega seonduvate ohtude ning andmesubjektide õiguste ja vabaduste kaitse vajaduse hindamist?

g. Kas kriteeriumid võimaldavad ja eeldavad füüsiliste isikute õigusi ja vabadusi ähvardavate ohtude arvessevõtmist?

…

5 ISIKUANDMETE TÖÖTLEMISE SEADUSLIKKUS

a. Kas kriteeriumid eeldavad, et konkreetsete töötlemistoimingute puhul kontrollitakse töötlemistoimingute seaduslikkust töötlemise eesmärgi ja vajalikkuse seisukohast?

b. Kas kriteeriumid eeldavad konkreetsete töötlemistoimingute õigusliku aluse kõigi nõuete kontrollimist?

6 PÕHIMÕTTED, ARTIKKEL 5

a. Kas kriteeriumide puhul on nõuetekohaselt arvesse võetud artikli 5 kohaseid isikuandmete kaitse põhimõtteid?

b. Kas kriteeriumid eeldavad konkreetse hindamise objekti kindlaksmääramisel selle tõendamist, et kogutud on võimalikult vähe andmeid?

…

7 VASTUTAVATE TÖÖTLEJATE JA VOLITATUD TÖÖTLEJATE ÜLDISED KOHUSTUSED

a. Kas kriteeriumid eeldavad tõendit vastutavate töötlejate ja volitatud töötlejate vaheliste lepinguliste suhete kohta?

b. Kas vastutavate töötlejate ja volitatud töötlejate vahelisi lepingulisi suhteid tuleb hinnata?

c. Kas kriteeriumide puhul on arvesse võetud vastutava töötleja IV peatükist tulenevaid kohustusi?

d. Kas kriteeriumid eeldavad tõendit selle kohta, et vastutava kontrollija poolt artikli 24 lõike 1 kohaselt rakendatud tehnilised ja korralduslikud meetmed on läbi vaadatud ja neid on ajakohastatud?

e. Kas kriteeriumidega kontrollitakse seda, kas organisatsioon on hinnanud, kas tuleks ametisse määrata andmekaitseametnik, nagu on nõutud artiklis 37? Kui see on asjakohane, kas andmekaitseametnik täidab artiklites 37–39 esitatud nõudeid?

f. Kas kriteeriumid tagavad, et nõutakse isikuandmete töötlemise toimingute registreerimist vastavalt artikli 30 lõikele 5 ja et registreerimisel on artikli 30 nõudeid asjakohaselt arvesse võetud?

8 ANDMESUBJEKTIDE ÕIGUSED

a. Kas kriteeriumide puhul on nõuetekohaselt arvesse võetud andmesubjekti õigust teabele ja nõutud asjakohaste meetmete rakendamist?

b. Kas kriteeriumid eeldavad, et andmesubjektidele antakse piisav või isegi ulatuslikum juurdepääs oma andmetele ja kontroll nende andmete üle, sealhulgas seoses andmete ülekantavusega?

c. Kas kriteeriumid eeldavad selliste meetmete paikapanemist, millega nähakse ette võimalus sekkuda töötlemistoimingusse, et tagada andmesubjektide õigused ja võimaldada andmeid parandada, kustutada või piirata?

…

9 FÜÜSILISTE ISIKUTE ÕIGUSI JA VABADUSI ÄHVARDAVAD OHUD

a. Kas kriteeriumid võimaldavad ja eeldavad, et hinnatakse füüsiliste isikute õigusi ja vabadusi ähvardavaid ohte?

b. Kas kriteeriumidega nähakse ette tunnustatud riskihindamismetoodika või eeldatakse selle olemasolu? Kui see on asjakohane, kas selline metoodika on proportsionaalne?

c. Kas kriteeriumid võimaldavad ja eeldavad, et hinnatakse kavandatavate töötlemistoimingute mõju füüsiliste isikute õigustele ja vabadustele?

d. Kas kriteeriumid eeldavad eelnevaid konsultatsioone seoses allesjäänud ohtudega, mida ei ole võimalik leevendada, toetudes andmekaitsealase mõjuhinnangu tulemustele?

10 KAITSET TAGAVAD TEHNILISED JA KORRALDUSLIKUD MEETMED

a. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse töötlemistoimingute konfidentsiaalsus?

b. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse töötlemistoimingute usaldusväärsus?

c. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse töötlemistoimingute kättesaadavus?

d. Kas kriteeriumid eeldavad, et kohaldatakse meetmeid, millega tagatakse töötlemistoimingute läbipaistvus seoses järgmiste aspektidega:

e. vastutus

f. andmesubjekti õigused

g. konkreetsete töötlemistoimingute hindamine, nt algoritmide läbipaistvus?

h. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse andmesubjektide õigused, nt võimalus anda teavet või andmeid üle kanda?

i. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega nähakse ette võimalus sekkuda töötlemistoimingusse, et tagada andmesubjektide õigused ja võimaldada andmeid parandada, kustutada või piirata?

j. Kas kriteeriumid eeldavad, et kohaldatakse meetmeid, millega nähakse ette võimalus sekkuda töötlemistoimingusse, et süsteemi või toimingut parandada või kontrollida?

k. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse võimalikult väheste andmete kogumine, näiteks andmete andmesubjektist lahtisidumise või eraldamise, anonüümimise, pseudonüümimise või andmesüsteemide isoleerimise kaudu?

l. Kas kriteeriumid eeldavad tehnilisi meetmeid vaikimisi andmetekaitse rakendamiseks?

m. Kas kriteeriumid eeldavad tehnilisi ja korralduslikke meetmeid lõimitud andmekaitse rakendamiseks, nt isikuandmete kaitse haldamise süsteemi loomist, et andmekaitse nõuete täitmist tõendada, kontrollida ja tagada ning sellest teavitada?

n. Kas kriteeriumid eeldavad, et kohaldatakse tehnilisi ja korralduslikke meetmeid, millega tagatakse asjakohane korrapärane koolitus ja õpe personalile, kellel on isikuandmetele pidev või regulaarne juurdepääs?

o. Kas kriteeriumid eeldavad läbivaatamismeetmeid?

p. Kas kriteeriumid eeldavad enesehindamist/siseauditit?

q. Kas kriteeriumid eeldavad meetmeid, millega tagada, et isikuandmetega seotud rikkumisest teatamise kohustust täidetakse õigeaegselt ja nõuetekohases ulatuses?

r. Kas kriteeriumid eeldavad, et paika on pandud juhtumite haldamise menetlused ja et neid kontrollitakse?

s. Kas kriteeriumid eeldavad eraelu puutumatust ja tehnoloogiat käsitlevate teemade arengu jälgimist ja vajaduse korral süsteemi ajakohastamist?

…

11 MUUD SPETSIIFILISED ISIKUANDMETE KAITSET SOODUSTAVAD TEGURID

a. Kas kriteeriumid eeldavad isikuandmete kaitset tõhustavate vahendite rakendamist? See võib hõlmata kriteeriume, mis eeldavad isikuandmete kaitse tõhustamist, eemaldades isikuandmed ja/või isikuandmete kaitsega seotud ohud või nende hulka vähendades.

- *Näide. Kriteeriumid, mis nõuavad seostamatuse suurendamist, kasutades selleks organisatsioonikeskse identiteedihalduse asemel kasutajakeskset identiteedihaldust, näiteks atribuudipõhist mandaati, võtaksid arvesse andmekaitset tõhustavat vahendit.*

b. Kas kriteeriumid eeldavad andmesubjektide suuremat kontrolli, et hõlbustada enesemääramist ja valikute tegemist?

…

12 KRITEERIUMID, MILLE ALUSEL TÕENDADA ISIKUANDMETE EDASTAMISEKS VAJALIKE ASJAKOHASTE KAITSEMEETMETE OLEMASOLU

Kriteeriume käsitletakse artikli 42 lõike 2 kohta koostatavates suunistes.

13 TÄIENDAVAD KRITEERIUMID, MIDA KOHALDATAKSE EUROOPA ANDMEKAITSEPITSERI SUHTES

a. Kas kriteeriumidega kavatsetakse hõlmata kõiki liikmesriike?

b. Kas kriteeriumid võimaldavad arvesse võtta liikmesriikide andmekaitsealaseid õigusakte või stsenaariume?

c. Kas kriteeriumid eeldavad konkreetsete hindamise objektide hindamist liikmesriikide sektoripõhiste isikuandmete kaitset käsitlevate õigusaktide seisukohast?

d. Kas kriteeriumid eeldavad, et vastutav töötleja või volitatud töötleja annab andmesubjektidele ja huvitatud isikutele liikmesriikide keeltes teavet järgmiste aspektide kohta:

e. töötlemistoiming / hindamise objekt

f. töötlemistoimingu / hindamise objekti dokumenteerimine

g. hindamise tulemused?

…

14 ÜLDISED HINDAMISKRITEERIUMID

a. Kas kriteeriumid hõlmavad sertifitseerimismehhanismi kogu kohaldamisala (s.t kriteeriumid on terviklikud), et anda piisav tagatis sertifitseerimise usaldusväärsuse kohta?

- *Näide. Kui sertifitseerimismehhanismi kohaldamisala on seotud tervishoiualaste töötlemistoimingutega, tuleks isikuandmete kaitse kõrge taseme tagamiseks määrata kindlaks kriteeriumid, millega nähakse ette näiteks põhjalik hindamine ning lõimprivaatsuse ja privaatsuse vaikesätetega seotud põhimõtete kohaldamine.*

b. Kas kriteeriumid on proportsionaalsed sertifitseerimismehhanismi kohaldamisalasse kuuluva töötlemistoimingu mahu, teabe tundlikkuse ja töötlemisega kaasnevate ohtudega?

c. Kas on tõenäoline, et kriteeriumid parandavad seda, kuidas vastutavad töötlejad ja volitatud töötlejad isikuandmete kaitse nõudeid täidavad?

d. Kas andmesubjektide õigus teabele paraneb ja kas neile antakse ülevaade, millised on soovitud tulemused?