
# Pamatnostādnes 1/2018 sertifikācijai un sertifikācijas kritēriju noteikšanai saskaņā ar Regulas 42. un 43. pantu

**Versija 3.0**

**2019. gada 4. jūnijs**

Translations proofread by EDPB Members.
This language version has not yet been proofread.

pieņemts

# Versijas vēsture

| | | |
|---|---|---|
| Versija 3.0 | 2019. gada 4. jūnijs | 2. pielikuma iekļaušana (2. pielikuma versija 2.0, kas pieņemta 2019. gada 4. jūnijā pēc sabiedriskas apspriešanās) |
| Versija 2.1 | 2019. gada 9. aprīlis | Pamatnostādņu kļūdu labojuma (45. punkts) pieņemšana |
| Versija 2.0 | 2019. gada 23. janvāris | Pamatnostādņu pieņemšana pēc sabiedriskas apspriešanās — tajā pašā datumā sabiedriskai apspriešanai tika pieņemts 2. pielikums (versija 1.0) |
| Versija 1.0 | 2018. gada 25. maijs | Pamatnostādņu pieņemšana sabiedriskai apspriešanai |

# Satura rādītājs

**Eiropas Datu aizsardzības kolēģija,**

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk tekstā — VDAR),

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, ko groza ar EEZ Apvienotās komitejas lēmumu Nr. 154/2018 (2018. gada 6. jūlijs),

ņemot vērā tās 2018. gada 25. maija reglamenta 12. un 22. punktu,

ņemot vērā sabiedriskās apspriešanas par pamatnostādnēm, kas norisinājās no 2018. gada 30. maija līdz 2018. gada 12. jūlijam, un sabiedriskās apspriešanas par 2. pielikumu, kas norisinājās no 2019. gada 15. februāra līdz 29. martam, rezultātus saskaņā ar VDAR 70. panta 4. punktu,

**IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.**

# 1 IEVADS

1. Vispārīgā datu aizsardzības regula (Regula 2016/279, turpmāk tekstā — VDAR vai Regula) nodrošina modernizētu, pārskatatbildību un pamattiesības ievērojošu sistēmu datu aizsardzībai Eiropā. Šīs jaunās sistēmas pamatā ir virkne pasākumu, kas veicina atbilstību VDAR noteikumiem. Tajos ietilpst obligātas prasības konkrētos apstākļos (tostarp datu aizsardzības speciālista iecelšana un datu aizsardzības ietekmes novērtējumu veikšana), kā arī brīvprātīgi pasākumi, piemēram, rīcības kodeksi un sertifikācijas mehānismi.

2. Pirms VDAR pieņemšanas 29. panta darba grupa secināja, ka sertifikācijai varētu būt nozīmīga loma datu aizsardzības pārskatatbildības sistēmā.1 Lai sertifikācija varētu sniegt uzticamus pierādījumus par datu aizsardzības ievērošanu, vajadzētu būt skaidriem noteikumiem, kuros izklāstītas sertifikācijas nodrošināšanas prasības.2 VDAR 42. pantā sniegts šādu noteikumu izstrādei nepieciešamais juridiskais pamats.

3. VDAR 42. panta 1. punktā noteikts, ka:

   “Dalībvalstis, uzraudzības iestādes, kolēģija un Komisija mudina, jo īpaši Savienības līmenī, izveidot datu aizsardzības sertifikācijas mehānismus un datu aizsardzības zīmogus un marķējumus, lai uzskatāmi parādītu, ka apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst šai regulai. Ņem vērā mikrouzņēmumu, mazo un vidējo uzņēmumu konkrētās vajadzības”.

[1] 29. panta darba grupas Atzinums 3/2010 par pārskatatbildības principu, WP173, 2010. gada 13. jūlijs, 69.-71. punkts.
[2] 29. panta darba grupas Atzinums 3/2010 par pārskatatbildības principu, WP173, 69. punkts.

4. Sertifikācijas mehānismi3 var uzlabot pārredzamību datu subjektiem, kā arī uzņēmumu attiecības ar uzņēmumiem, piemēram, starp pārziņiem un apstrādātājiem. VDAR 100. apsvērumā noteikts, ka sertifikācijas mehānismu izstrāde var uzlabot pārredzamību un atbilstību Regulai, kā arī ļaut datu subjektiem novērtēt attiecīgo produktu un pakalpojumu datu aizsardzības līmeni.4

5. Ar VDAR neievieš tiesības vai pienākumu pārziņiem un apstrādātājiem veikt sertifikāciju; saskaņā ar 42. panta 3. punktu sertifikācija ir brīvprātīgs process, kas palīdz uzskatāmi parādīt atbilstību VDAR. Dalībvalstis un uzraudzības iestādes tiek aicinātas iedrošināt sertifikācijas mehānismu izstrādi un noteiks ieinteresēto personu iesaisti sertifikācijas procesā un dzīves ciklā.

6. Turklāt apstiprināto sertifikācijas mehānismu ievērošana ir faktors, kas uzraudzības iestādēm ir jāņem vērā kā atbildību pastiprinošs vai mīkstinošs apstāklis, lemjot par administratīvā naudas soda uzlikšanu un par naudas soda apmēru (83. panta 2. punkta j) apakšpunkts).5

## 1.1 Pamatnostādņu piemērošanas joma

7. Šo pamatnostādņu piemērošanas joma ir ierobežota; tās nav saskaņā ar VDAR veicamas sertifikācijas procesa rokasgrāmata. Šo pamatnostādņu galvenais mērķis ir noteikt vispārējās prasības un kritērijus, kas var būt būtiski visa veida sertifikācijas mehānismiem, kuri tiek izsniegti saskaņā ar VDAR 42. un 43. pantu. Šim nolūkam pamatnostādnēs:

   - apskatīts sertifikācijas kā pārskatatbildības instrumenta pamatojums;
   - izskaidroti 42. un 43. pantā sniegto sertifikācijas noteikumu galvenie jēdzieni; un
   - izskaidrots, ko var sertificēt saskaņā ar 42. un 43. pantu, kā arī sertifikācijas nolūks;
   - veicināts jēgpilns, nepārprotams, pēc iespējas reproducējams un salīdzināms sertifikācijas rezultāts neatkarīgi no sertificētāja (salīdzināmība).

8. VDAR ļauj dalībvalstīm un uzraudzības iestādēm ieviest 42. un 43. pantu dažādos veidos. Pamatnostādnēs sniegti ieteikumi 42. un 43. panta normu interpretācijai un ieviešanai, un tās palīdzēs dalībvalstīm, uzraudzības iestādēm un valstu akreditācijas struktūrām izveidot konsekventāku un saskaņotāku pieeju sertifikācijas mehānismu īstenošanai saskaņā ar VDAR.

9. Šajās pamatnostādnēs ietvertais padoms būs noderīgs:

   - kompetentajām uzraudzības iestādēm un Eiropas Datu aizsardzības kolēģijai (EDAK), apstiprinot sertifikācijas kritērijus saskaņā ar 42. panta 5. punktu, 58. panta 3. punkta f) apakšpunktu un 70. panta 1. punkta o) apakšpunktu;

[3] Šajās pamatnostādnēs sertifikācijas mehānismi un datu aizsardzības zīmogi un marķējumi kopā tiek saukti par "sertifikācijas mehānismiem", skatīt 1.3.2. sadaļu.
[4] VDAR 100. apsvērumā noteikts, ka sertifikācijas mehānismu izveide būtu jāiedrošina, lai uzlabotu "pārredzamību un šīs regulas ievērošanu, [..] ļautu datu subjektam ātri novērtēt datu aizsardzības līmeni saistībā ar konkrētiem produktiem un pakalpojumiem".
[5] Skatīt 29. panta darba grupas Pamatnostādnes administratīvo naudas sodu piemērošanai un noteikšanai Regulas 2016/679 vajadzībām (WP 253).

- sertifikācijas struktūrām, izstrādājot un pārskatot sertifikācijas kritērijus, pirms iesniegšanas apstiprināšanai kompetentajā uzraudzības iestādē saskaņā ar 42. panta 5. punktu;
- EDAK, apstiprinot Eiropas datu aizsardzības zīmogu saskaņā ar 42. panta 5. punktu un 70. panta 1. punkta o) apakšpunktu;
- uzraudzības iestādēm, izstrādājos savus sertifikācijas kritērijus;
- Eiropas Komisijai, kura ir tiesīga pieņemt deleģētos aktus nolūkā precizēt prasības, kas jāņem vērā sertifikācijas mehānismos saskaņā ar 43. panta 8. punktu;
- EDAK, sniedzot Eiropas Komisijai atzinumu par sertifikācijas prasībām saskaņā ar 70. panta 1. punkta q) apakšpunktu un 43. panta 8. punktu;
- valsts akreditācijas struktūrām, kurām jāņem vērā sertifikācijas kritēriji sertifikācijas struktūru akreditācijā atbilstoši EN-ISO/IEC 17065/2012 un papildu prasībām saskaņā ar 43. pantu; un
- pārziņiem un apstrādātājiem, nosakot savu atbilstības VDAR nodrošināšanas stratēģiju un apsverot sertifikāciju kā atbilstības pierādīšanas līdzekli.

10. EDAK publicēs atsevišķas pamatnostādnes par kritēriju noteikšanu, lai apstiprinātu sertifikācijas mehānismus kā nosūtīšanas uz trešām valstīm un starptautiskām organizācijām instrumentus atbilstīgi 42. panta 2. punktam.

## 1.2 Sertifikācijas nolūks saskaņā ar VDAR

11. 42. panta 1. punktā noteikts, ka sertifikācijas mehānismus izstrādā "lai uzskatāmi parādītu, ka apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst šai regulai".
12. VDAR ir piemērs kontekstam, kurā apstiprinātos sertifikācijas mehānismus var izmantot kā elementu, lai uzskatāmi parādītu, ka tiek ievēroti pārziņu un apstrādātāju pienākumi attiecībā uz:
    - atbilstošu tehnisku un organizatorisku pasākumu īstenošanu un uzskatāmu parādīšanu, kā minēts 24. panta 1. un 3. punktā, 25. pantā un 32. panta 1. un 3. punktā;
    - pietiekamām garantijām kā minēts 28. panta 5. punktā — (apstrādātājs pārzinim) 1. punktā un (apakšapstrādātājs apstrādātājam) 4. punktā.
13. Tā kā sertifikācija pati par sevi nepierāda atbilstību, bet drīzāk veido elementu, ko var izmantot, lai uzskatāmi parādītu atbilstību, tā būtu jāveic pārredzamā veidā. Atbilstības uzskatāmai parādīšanai ir nepieciešami apliecinoši dokumenti, jo īpaši rakstiski ziņojumi, kuros ne tikai atkārto, bet arī apraksta, kā kritēriji ir izpildīti, un, ja tie sākotnēji nav izpildīti, apraksta veiktās korekcijas un koriģējošās darbības un to piemērotību, tādējādi sniedzot sertifikācijas piešķiršanas un uzturēšanas iemeslus. Tas ietver konkrētā lēmuma par sertifikāta piešķiršanu, atjaunošanu vai atsaukšanu izklāstu. Tajā būtu jānorāda iemesli, argumenti un pierādījumi, kas izriet no kritēriju piemērošanas, kā arī secinājumi, spriedumi vai slēdzieni, kas izriet no sertifikācijas laikā iegūtajiem faktiem vai premisām.

## 1.3 Galvenie jēdzieni

14. Šajā sadaļā ir apskatīti 42. un 43. pantā ietvertie galvenie jēdzieni. Šajā analīzē tiek veidota izpratne par pamata terminiem un sertifikācijas piemērošanas jomu saskaņā ar VDAR.

### 1.3.1 "Sertifikācijas" interpretācija

15. VDAR "sertifikācija" nav definēta. Starptautiskā Standartizācijas organizācija (ISO) vispārīgi definē sertifikāciju kā "neatkarīgas struktūras rakstveida apliecinājuma (sertifikāta) izsniegšanu, apliecinot, ka attiecīgais produkts, pakalpojums vai sistēma atbilst konkrētām prasībām". Sertifikāciju dēvē arī par "trešās personas atbilstības novērtējumu", un sertifikācijas struktūras dēvē arī par "atbilstības novērtējuma struktūrām" (CAB). Standartā EN-ISO/IEC 17000:2004 — Atbilstības novērtēšana — Vārdnīca un vispārīgie principi (uz ko atsaucas ISO17065) sertifikācija ir definēta šādi: "trešās personas apliecinājums... attiecībā uz produktiem, procesiem un pakalpojumiem".

16. Apliecinājums ir "paziņojums, kas balstīts uz lēmumu, kurš pieņemts, izskatot, vai ir pierādīta konkrētu prasību izpilde" (5.2. sadaļa, ISO 17000:2004).

17. Saistībā ar sertifikāciju saskaņā ar VDAR 42. un 43. pantu sertifikācija attiecas uz trešās personas apliecinājumu, kas saistīts ar pārziņu un apstrādātāju veiktajām apstrādes darbībām.

### 1.3.2 Sertifikācijas mehānismi, zīmogi un marķējumi

18. VDAR "sertifikācijas mehānismi, zīmogi vai marķējumi" nav definēti un šie termini tiek lietoti kopā. Sertifikāts ir atbilstības apliecinājums. Zīmogu vai marķējumu var izmantot, lai apzīmētu sekmīgu sertifikācijas procedūras pabeigšanu. Zīmogs vai marķējums parasti apzīmē logotipu vai simbolu, kura esība (papildus sertifikātam) norāda, ka sertifikācijas procedūrā sertifikācijas objekts ir ticis neatkarīgi novērtēts un atbilst konkrētajām normatīvajos dokumentos, piemēram, noteikumos, standartos vai tehniskajās specifikācijās, noteiktajām prasībām. Šīs prasības saistībā ar sertifikāciju VDAR ietvaros ir noteiktas papildu prasībās, kas papildina sertifikācijas struktūru akreditācijas noteikumus saskaņā ar EN-ISO/IEC 17065/2012 un sertifikācijas kritērijiem, ko apstiprinājusi kompetentā uzraudzības iestāde vai kolēģija. Sertifikātu, zīmogu vai marķējumu VDAR nolūkos var izsniegt tikai pēc tam, kad akreditēta sertifikācijas struktūra vai kompetentā uzraudzības iestāde ir veikusi neatkarīgu pierādījumu novērtējumu, apliecinot, ka sertifikācijas kritēriji ir izpildīti.

19. Tabulā sniegts vispārīgs sertifikācijas procesa piemērs.

| Pārzina vai apstrādātāja pieteikuma iesniegšana | Sertifikācijas struktūras veikti oficiāli pārbaude | Novērtējums Iepriekšēja izvērtēšana | Novērtējums ToE izvērtēšana | Novērtējums Rezultātu apstiprināšana | Sertifikācijas uzraudzības iestādei iesniedzamā informācija | Sertifikācija | Uzraudzība | Sertificēta otrjoņošana |
|---|---|---|---|---|---|---|---|---|
| Vai novērtēšanas mērķis (ToE) apraksts ir nepārprotams un pilnīgs, iekļaujot saskarnes? | Vai ToE apraksts ir pieņemams? | Kādi ir piemērojamie kritēriji? | Vai ToE atbilst kritērijiem? | Vai ir norādīti visi būtiskie kritēriji, kuri atspoguļo ToE? | Vai ir norādīti sertifikāta piešķiršanas vai atsaukšanas kritēriji? | Vai sertifikātu var piešķirt? | Vai ToE joprojām atbilst kritērijiem? | Vai apstrāde joprojām atbilst sertifikācijas kritērijiem? |
| Vai var sniegt pierādījumi ToE apstrādes rezultātiem? | Vai visi dokumenti ir pilnīgi un aktuālo informāciju saturoši? | Kādas ir piemērojamās izvērtēšanas metodes? | Vai ToE dokumentācija ir pareiza? | Vai izvērtēšana ir dokumenteta pietiekamā apmērā? | | Vai ziņojumi ir gatavi publicēšanai? | Vai sertifikāts/zīmogs/uzticības zīme tiek izmantoti pareizi? | Vai attīstības izmaiņas pieņemti noraidītas? |
| 42. panta 6. punkts | 43. panta 4. punkts | 43. panta 4. punkts | 42. panta 5. punkts, 42. panta 4. punkts | 43. panta 4. punkts | 43. panta 1. un 5. punkts | 43. panta 1. punkts, 42. panta 7. punkts | 42. panta 7. punkts | 42. panta 7. punkts |

# 2 UZRAUDZĪBAS IESTĀŽU LOMA

20. 42. panta 5. punktā paredzēts, ka sertifikātus izsniedz akreditēta sertifikācijas struktūra vai kompetentā uzraudzības iestāde. VDAR nav uzlikts uzraudzības iestādēm obligāts pienākums veikt sertifikāciju. Tā vietā VDAR pieļauti vairāki modeļi. Piemēram, uzraudzības iestāde var lemt par vienu vai vairākām šādām iespējām:

   - pati izsniegt sertifikātus saskaņā ar savu sertifikācijas sistēmu;
   - pati izsniegt sertifikātus saskaņā ar savu sertifikācijas sistēmu, taču deleģēt visu vai daļu novērtēšanas procesa trešām personām;
   - izveidot savu sertifikācijas sistēmu un uzticēt sertifikācijas struktūrām sertifikācijas procedūru; un
   - mudināt tirgu izstrādāt sertifikācijas mehānismus.

21. Uzraudzības iestādei būs arī jāapsver tās funkcija valsts līmenī pieņemto lēmumu par akreditācijas mehānismiem kontekstā, jo īpaši, ja uzraudzības iestāde pati ir pilnvarota akreditēt sertifikācijas struktūras saskaņā ar VDAR 43. panta 1. punktu. Tādējādi katra uzraudzības iestāde noteiks, kādu pieeju izmantot, īstenojot sertifikācijas plašo nodomu, kā paredzēts VDAR. Tas tiks noteikts ne tikai saistībā ar 57. un 58. pantā minētajiem uzdevumiem un pilnvarām, bet arī attiecībā uz sertifikācijas uzskaiti kā faktoru, ko ņem vērā, piemērojot administratīvos naudas sodus, un kā līdzekli atbilstības uzskatāmai parādīšanai kopumā.

## 2.1 Uzraudzības iestāde kā sertifikācijas struktūra

22. Ja uzraudzības iestāde izvēlas veikt sertifikāciju, tai būs rūpīgi jāizvērtē tās funkcija attiecībā uz VDAR ietvaros uzticētajiem uzdevumiem. Veicot savu funkciju, iestādei būtu jābūt

pārredzamai. Lai izvairītos no jebkādiem iespējamiem interešu konfliktiem, tai būs īpaši jāizvērtē ar izmeklēšanu un izpildi saistīto pilnvaru nodalīšana.

23. Rīkojoties kā sertifikācijas struktūra, uzraudzības iestādei būs jānodrošina pienācīga sertifikācijas mehānisma izveide un jāizstrādā savi vai jāpieņem sertifikācijas kritēriji. Turklāt katrai uzraudzības iestādei, kura izdod sertifikātus, ir pienākums tos periodiski pārskatīt (57. panta 1. punkta o) apakšpunkts), kā arī pilnvaras tos atsaukt, ja sertifikācijas prasības nav izpildītas vai vairs netiek pildītas (58. panta 2. punkta h) apakšpunkts). Lai izpildītu šīs prasības, ir lietderīgi izveidot sertifikācijas procedūru un procesa prasības, un, ja nav noteikts citādi, piemēram, saskaņā ar valsts tiesību aktiem, noslēgt juridiski izpildāmu nolīgumu par sertifikācijas darbību nodrošināšanu ar atsevišķo pieteikuma iesniedzēju organizāciju. Jānodrošina, ka šajā sertifikācijas nolīgumā pieprasīts, lai pieteikuma iesniedzējs izpilda vismaz sertifikācijas kritērijus, tostarp pasākumus, kas nepieciešami, lai veiktu izvērtēšanu, uzraudzītu kritēriju izpildi un periodisku pārskatīšanu, tostarp piekļuvi informācijai un/vai telpām, dokumentāciju un ziņojumu un rezultātu publicēšanu, kā arī sūdzību izskatīšanu. Turklāt ir paredzams, ka uzraudzības iestāde papildus prasībām, kas noteiktas 43. panta 2. punktā, ievēros sertifikācijas struktūru akreditācijas pamatnostādnēs noteiktās prasības.

## 2.2 Uzraudzības iestādes papildu uzdevumi saistībā ar sertifikāciju

24. Dalībvalstīs, kurās sertifikācijas struktūras kļūst aktīvas, uzraudzības iestādei ir pilnvaras un uzdevumi neatkarīgi no savām darbībām:

- novērtēt sertifikācijas sistēmas kritērijus un sagatavot lēmuma projektu (42. panta 5. punkts);
- informēt kolēģiju par lēmuma projektu, ja tā plāno apstiprināt sertifikācijas kritērijus (64. panta 1. punkta c) apakšpunkts, 64. panta 7. punkts) un izskatīt kolēģijas atzinumu (64. panta 1. punkta c) apakšpunkts un 70. panta 1. punkta t) apakšpunkts);
- apstiprināt sertifikācijas kritērijus (58. panta 3. punkta f) apakšpunkts), pirms var veikt akreditāciju un sertifikāciju (42. panta 5. punkts un 43. panta 2. punkta b) apakšpunkts);
- publicēt sertifikācijas kritērijus (43. panta 6. punkts);
- darboties kā kompetentajai iestādei attiecībā uz ES mēroga sertifikācijas sistēmām, kā rezultātā var iegūt EDAK apstiprinātus Eiropas datu aizsardzības zīmogus (42. panta 5. punkts un 70. panta 1. punkta o) apakšpunkts); un
- uzdot sertifikācijas struktūrai: a) neizdot sertifikātus vai b) atsaukt sertifikātus, ja sertifikācijas prasības (sertifikācijas procedūras vai kritēriji) nav izpildītas vai vairs netiek pildītas (58. panta 2. punkta h) apakšpunkts).

25. VDAR uzdod uzraudzības iestādei apstiprināt sertifikācijas kritērijus, bet ne izstrādāt kritērijus. Lai apstiprinātu sertifikācijas kritērijus saskaņā ar 42. panta 5. punktu, uzraudzības iestādei būtu skaidri jāapzinās, ko sagaidīt, jo īpaši attiecībā uz piemērošanas jomu un saturu, uzskatāmi parādot atbilstību VDAR, kā arī attiecībā uz tās uzdevumu uzraudzīt regulas

noteikumu piemērošanu un panākt to izpildi. Pielikumā ir sniegti norādījumi nolūkā nodrošināt saskaņotu pieeju apstiprināšanas kritēriju novērtēšanā.

26. Saskaņā ar 43. panta 1. punktu sertifikācijas struktūrām pirms sertifikātu izsniegšanas vai atjaunošanas jāinformē savu uzraudzības iestādi, lai kompetentā uzraudzības iestāde varētu īstenot savas korektīvās pilnvaras saskaņā ar 58. panta 2. punkta h) apakšpunktu. Turklāt 43. panta 5. punktā ir prasīts sertifikācijas struktūrām norādīt kompetentajai uzraudzības iestādei iemeslus, kādēļ pieprasītais sertifikāts ir piešķirts vai atsaukts. Lai gan VDAR ļauj uzraudzības iestādēm noteikt, kā šo informāciju operatīvi saņemt, atzīt, pārskatīt un apstrādāt (piemēram, tie var būt tehnoloģiski risinājumi, ar ko sertifikācijas struktūrām ļauj sniegt ziņojumus), var ieviest procesu un kritērijus sniegtās informācijas un ziņojumu apstrādei saskaņā ar 43. panta 1. punktu par katru sertifikācijas struktūras veiksmīgu sertifikācijas projektu. Pamatojoties uz šo informāciju, uzraudzības iestāde var izmantot savas pilnvaras uzdot sertifikācijas struktūrai atsaukt vai neizsniegt sertifikātu (58. panta 2. punkta h) apakšpunkts), kā arī uzraudzīt sertifikācijas prasību un kritēriju piemērošanu un panākt to izpildi saskaņā ar VDAR (57. panta 1. punkta a) apakšpunkts un 58. panta 2. punkta h) apakšpunkts). Tādējādi tiks veicināta saskaņota pieeja un salīdzināmība dažādu sertifikācijas struktūru sertifikācijā, kā arī informācijas par organizācijas sertifikācijas statusu pieejamība uzraudzības iestādēm.

# 3 SERTIFIKĀCIJAS STRUKTŪRAS FUNKCIJA

27. Sertifikācijas struktūras uzdevums ir izdot, pārskatīt, atjaunot un atsaukt sertifikātus (42. panta 5. un 7. punkts), pamatojoties uz sertifikācijas mehānismu un apstiprinātajiem kritērijiem (43. panta 1. punkts). Sertifikācijas struktūrai vai sertifikācijas sistēmas īpašniekam jānosaka un jāizstrādā sertifikācijas kritēriji un sertifikācijas procedūras, tostarp procedūras ievērošanas uzraudzībai, pārskatīšanai, sūdzību izskatīšanai un atsaukšanai. Sertifikācijas kritērijus pārskata akreditācijas procesa ietvaros, kurā ņemti vērā noteikumi un procedūras, saskaņā ar kuriem izdod sertifikātus, zīmogus vai marķējumus (43. panta 2. punkta c) apakšpunkts).

28. Lai panāktu akreditāciju saskaņā ar 43. pantu, sertifikācijas struktūrai ir jābūt sertifikācijas mehānismam un sertifikācijas kritērijiem. Būtiska ietekme uz sertifikācijas struktūras veiktajiem darbiem ir sertifikācijas kritēriju piemērošanas jomai un veidam, kas ietekmē sertifikācijas procedūras un otrādi. Konkrētiem kritērijiem, piemēram, var būt nepieciešamas konkrētas izvērtēšanas metodes, piemēram, uz vietas veiktas pārbaudes un kodeksa pārskatīšana. Šīs procedūras ir obligātas akreditācijai un tās sīkāk paskaidrotas akreditācijas pamatnostādnēs.

29. VDAR nosaka sertifikācijas struktūrai pienākumu sniegt uzraudzības iestādēm informāciju, jo īpaši par atsevišķiem sertifikātiem, kas nepieciešama, lai uzraudzītu sertifikācijas mehānisma piemērošanu (42. panta 7. punkts, 43. panta 5. punkts, 58. panta 2. punkta h) apakšpunkts).

# 4 SERTIFIKĀCIJAS KRITĒRIJU APSTIPRINĀŠANA

30. Sertifikācijas kritēriji ir neatņemama jebkura sertifikācijas mehānisma sastāvdaļa. Līdz ar to VDAR paredzēts, lai kompetentā uzraudzības iestāde apstiprinātu sertifikācijas mehānisma sertifikācijas kritērijus (42. panta 5. punkts un 43. panta 2. punkta b) apakšpunkts). Vai arī Eiropas datu aizsardzības zīmoga gadījumā sertifikācijas kritērijus apstiprina EDAK (42. panta 5. punkts un 70. panta 1. punkta o) apakšpunkts). Abi sertifikācijas kritēriju apstiprināšanas ceļi ir izskaidroti turpmāk.

31. EDAK atzīst šādus sertifikācijas kritēriju apstiprināšanas nolūkus:

- pienācīgi atspoguļot prasības un principus, kas skar fizisko personu aizsardzību attiecībā uz personas datu apstrādi, kā noteikts Regulā (ES) 2016/679; un
- veicināt konsekventu VDAR piemērošanu.

32. Apstiprinājums tiek piešķirts, pamatojoties uz to, ka VDAR prasība sertifikācijas mehānismam ļaut pārziņiem un apstrādātājiem uzskatāmi parādīt savu atbilstību VDAR, ir pilnībā atspoguļota sertifikācijas kritērijos.

## 4.1 Kompetentās uzraudzības iestādes veiktā kritēriju apstiprināšana

33. Sertifikācijas kritērijus apstiprina kompetentā uzraudzības iestāde pirms sertifikācijas struktūras akreditācijas procesa vai tā laikā. Apstiprinājums ir nepieciešams arī atjauninātām vai papildu sistēmām vai kritēriju kopumiem saskaņā ar ISO 17065 vienai un tai pašai sertifikācijas struktūrai pirms grozīto sertifikācijas mehānismu piemērošanas (42. panta 5. punkts un 43. panta 2. punkta b) apakšpunkts). Uzraudzības iestādes visus sertifikācijas kritēriju apstiprināšanas pieprasījumus izskata taisnīgā un nediskriminējošā veidā, ievērojot sabiedriski pieejamu procedūru, norādot vispārējos nosacījumus un apstiprināšanas procesa aprakstu.

34. Sertifikācijas struktūra var izsniegt sertifikātu konkrētā dalībvalstī tikai saskaņā ar kritērijiem, kurus apstiprinājusi uzraudzības iestāde šajā dalībvalstī. Citiem vārdiem sakot, sertifikācijas kritērijus apstiprina kompetentā uzraudzības iestāde, ja sertifikācijas struktūra vēlas piedāvāt sertifikāciju un iegūst akreditāciju. Eiropas mēroga sertifikācijas shēmas skatīt nākamajā sadaļā.

## 4.2 EDAK veiktā kritēriju apstiprināšana Eiropas datu aizsardzības zīmogam

35. Sertifikācijas struktūra var izsniegt sertifikātu arī saskaņā ar kritērijiem, kurus EDAK apstiprinājusi attiecībā uz Eiropas datu aizsardzības zīmogu. Sertifikācijas kritēriju, ko EDAK apstiprinājusi saskaņā ar 63. pantu, rezultātā var iegūt Eiropas datu aizsardzības zīmogu (42. panta 5. punkts). Ņemot vērā spēkā esošās sertifikācijas un akreditācijas konvencijas, EDAK atzīst, ka vajadzētu izvairīties no datu aizsardzības sertifikācijas tirgus sadrumstalotības. Tā atzīmē, ka 42. panta 1. punkts paredz dalībvalstīm, uzraudzības iestādēm, kolēģijai un Komisijai veicināt sertifikācijas mehānismu izveidi, jo īpaši Savienības līmenī.

### 4.2.1 Pieteikuma iesniegšana apstiprināšanai

36. Pieteikumu par kritēriju apstiprināšanu saskaņā ar 42. panta 5. punktu un 70. panta 1. punkta o) apakšpunktu jāiesniedz EDAK, izmantojot kompetento uzraudzības iestādi, un tajā būtu jānorāda sistēmas īpašnieka, kandidāta vai akreditētās sertifikācijas struktūras nodoms piedāvāt kritērijus sertifikācijas mehānismā, kas attiecas uz pārziņiem un apstrādātājiem visās dalībvalstīs. Kompetentā uzraudzības iestāde iesniegs EDAK projektu, ja uzskatīs, ka EDAK varētu apstiprināt šos kritērijus.

37. Izvēle par to, kur iesniegt pieteikumu kritēriju apstiprināšanai, atkarīga no sertifikācijas sistēmas īpašnieka vai sertifikācijas struktūras galvenās mītnes.

38. Ja sertifikācijas struktūra iesniedz pieteikumu, tā parasti jau būs iesniegusi akreditācijas pieteikumu vai to jau būs akreditējusi kompetentā uzraudzības iestāde vai tās dalībvalsts akreditācijas struktūra. Gadījumos, kad sertifikācijas struktūra jau ir akreditēta VDAR sertifikācijas mehānismam, apstiprināšanas process var tikt vienkāršots.

### 4.2.2 Eiropas datu aizsardzības zīmoga kritēriji

39. EDAK koordinēs novērtēšanas procesu un vajadzības gadījumā apstiprinās Eiropas datu aizsardzības zīmoga kritērijus. Novērtējumā tiks aplūkotas šādas jomas: kritēriju piemērošanas joma un piemērotība kopīgai sertifikācijai. Ja kritērijus apstiprina EDAK, sagaidāms, ka kompetentā uzraudzības iestāde ES sertifikācijas struktūras galvenajai mītnei izskatīs sūdzības par pašu mehānismu un informēs pārējās uzraudzības iestādes. Šī uzraudzības iestāde ir arī kompetenta īstenot pasākumus pret sertifikācijas struktūru. Attiecīgā gadījumā kompetentā uzraudzības iestāde informēs pārējās uzraudzības iestādes un EDAK.

40. Sertifikācijas kritērijiem, kas attiecas uz kopīgu sertifikāciju, piemēro ES mēroga prasības, un tiem būtu jānodrošina īpašs mehānisms šo prasību izpildei. Eiropas sertifikācijas mehānismiem jābūt paredzētiem izmantošanai visās dalībvalstīs. Pamatojoties uz 42. panta 5. punktu, Eiropas datu aizsardzības zīmoga mehānismam, kā arī tā kritērijiem jābūt individuāli pielāgojamiem tā, lai vajadzības gadījumā tie ņemtu vērā valsts nozarei specifiskus noteikumus, piemēram, datu apstrādei skolās, un jāparedz piemērošana Eiropas mērogā.

41. Piemēram: Starptautiska skola, kas piedāvā izglītības iespējas datu subjektiem Savienībā, atrodas dalībvalstī "A". Skola vēlas sertificēt savu tiešsaistes pieteikumu iesniegšanas procesu, izmantojot ES mēroga sertifikācijas sistēmu, lai iegūtu Eiropas datu aizsardzības zīmogu. Šī skola vēlas pieteikties apstrādes darbību sertifikātam, ko piedāvā dalībvalstī "B" bāzēta sertifikācijas struktūra, pamatojoties uz Eiropas datu aizsardzības zīmogu. Zīmoga kritērijiem, kas ir izstrādāti un dokumentēti attiecīgajā mehānismā, jāspēj ņemt vērā dalībvalstī "A" skolām piemērojamie noteikumi. Kritērijos būtu arī jāparedz, lai skolas tiešsaistes pieteikumu iesniegšanas procesā tiek sniegta informācija un ņemtas vērā piemērojamās dalībvalsts datu aizsardzības prasības, kas citās dalībvalstīs var atšķirties. Piemērs ir personas datu kopums, kas jāiesniedz pieteikumu vajadzībām, piem., bērnudārza

atzīmes vai testu rezultāti, atšķirīgi saglabāšanas periodi, finanšu vai biometrisko datu vākšana vai apstrāde, papildu apstrādes ierobežojumi.

- Vispārīgie kritēriji Eiropas datu aizsardzības zīmoga mehānisma apstiprināšanai ir šādi:
  - kolēģijas apstiprināti kritēriji;
  - piemērošana dažādās jurisdikcijās, vajadzības gadījumā atspoguļojot valsts juridiskās prasības un uz nozari attiecināmus noteikumus;

- saskaņoti kritēriji, kas ir individuāli pielāgojami, lai atspoguļotu valstu prasības;
  - sertifikācijas mehānisma apraksts ar norādēm;
  - sertifikācijas nolīgumi, kuros atzītas Eiropas mēroga prasības;
  - procedūras, ar ko nodrošina un sniedz valstu atšķirību risinājumus, kā arī nodrošina, ka zīmogs palīdz uzskatāmi parādīt atbilstību VDAR; un
  - to ziņojumu valoda, kas attiecas uz visām skartajām uzraudzības iestādēm.

42. Pielikumā iekļauti arī ieteikumi Eiropas datu aizsardzības zīmoga kritērijiem.

### 4.2.3 Akreditācijas funkcija

43. Kā minēts 4.2.1. punktā, ja kritēriji tiek atzīti par piemērotiem kopīgai sertifikācijai un kolēģija tos ir apstiprinājusi saskaņā ar 42. panta 5. punktu, tad sertifikācijas struktūras var tikt akreditētas veikt sertifikāciju saskaņā ar šiem kritērijiem Savienības līmenī.

44. Sistēmas, kuras paredzēts piedāvāt tikai konkrētās dalībvalstīs, nebūs ES zīmogu kandidāti. Eiropas datu aizsardzības zīmoga piemērošanas jomas akreditācijai būs nepieciešama akreditācija dalībvalstī, kurā atrodas tās sertifikācijas struktūras galvenā mītne, kas plāno izmantot sistēmu, t. i., būt atbildīga par sertifikātu izsniegšanu un tās struktūrvienību un meitasuzņēmumu sertifikācijas darbību pārvaldīšanu citās dalībvalstīs. Ja citi uzņēmumi vai biroji patstāvīgi pārvalda un veic sertifikācijas, katram no šiem uzņēmumiem vai birojiem nepieciešama atsevišķa akreditācija attiecīgajā dalībvalstī, kurā tie atrodas. Citiem vārdiem sakot, akreditācija ir nepieciešama tikai sertifikācijas struktūras galvenās mītnes dalībvalstī gadījumos, kad tikai galvenā mītne izsniedz sertifikātus. Turpretim, ja sertifikācijas struktūras citi uzņēmumi arī izdod sertifikātus, šiem uzņēmumiem arī jābūt akreditētiem.

45. Līdz ar to, ja sertifikācijas struktūra nav akreditēta sertificēt saskaņā ar Eiropas datu aizsardzības zīmogu, tad EDAK apstiprinātos kritērijus nevar izmantot un zīmogu nevar piedāvāt.

# 5 SERTIFIKĀCIJAS KRITĒRIJU IZSTRĀDE

46. Ar VDAR ir izveidota sistēma sertifikācijas kritēriju izstrādei. Tā kā pamatprasības attiecībā uz sertifikācijas procedūru ir aplūkotas 42. un 43. pantā, vienlaikus paredzot svarīgākos kritērijus sertifikācijas procedūrām, sertifikācijas kritēriju pamatā jābūt VDAR principiem un noteikumiem un tiem jāveicina pārliecība, ka tie ir izpildīti.

47. Sertifikācijas kritēriju izstrādē galvenā uzmanība būtu jāpievērš sertifikācijas kritēriju pārbaudes iespējamībai, nozīmīgumam un piemērotībai uzskatāmi parādīt atbilstību regulai. Sertifikācijas kritēriji būtu jāformulē tā, lai tie būtu skaidri un saprotami, kā arī tiem jābūt praktiski piemērojamiem.

48. Izstrādājot sertifikācijas kritērijus, vajadzības gadījumā cita starpā ņem vērā šādus atbilstības aspektus, kas palīdz veikt apstrādes darbības novērtējumu:

- apstrādes likumību saskaņā ar 6. pantu;
- datu apstrādes principus saskaņā ar 5. pantu;
- datu subjektu tiesības saskaņā ar 12. līdz 23. pantu;
- pienākumu informēt par datu pārkāpumiem saskaņā ar 33. pantu;
- integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma pienākumu saskaņā ar 25. pantu;
- vai ir veikts datu aizsardzības ietekmes novērtējums saskaņā ar 35. panta 7. punkta d) apakšpunktu, ja tāds ir piemērojams; un
- ieviestos tehniskos un organizatoriskos pasākumus saskaņā ar 32. pantu.

49. Tas, cik lielā mērā šie apsvērumi ir atspoguļoti kritērijos, var atšķirties atkarībā no sertifikācijas piemērošanas jomas, kas var ietvert apstrādes darbības veidu(-us) un sertifikācijas jomu (piemēram, veselības nozare).

## 5.1 Ko var sertificēt saskaņā ar VDAR?

50. EDAK uzskata, ka VDAR nodrošina plašu piemērošanas jomu attiecībā uz to, ko var sertificēt saskaņā ar VDAR, kamēr galvenā uzmanība ir pievērsta tam, lai palīdzētu uzskatāmi parādīt, ka apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst šai regulai (42. panta 1. punkts).

51. Izvērtējot apstrādes darbību, attiecīgā gadījumā ņem vērā trīs galvenos komponentus:

1. personas dati (VDAR materiālā piemērošanas joma);
2. tehniskās sistēmas — infrastruktūra, piemēram, aparatūra un programmatūra, kuru izmanto personas datu apstrādei; un
3. procesi un procedūras, kas saistīti ar apstrādes darbību(-ām).

52. Katru apstrādes darbībās izmantoto komponentu novērtē atbilstoši noteiktajiem kritērijiem. Iespējama vismaz četru dažādu nozīmīgu faktoru ietekme: 1) pārziņa vai apstrādātāja organizācija un juridiskā struktūra; 2) apstrādes darbībā(-ās) iesaistītais departaments, vide un cilvēki; 3) novērtējamo elementu tehniskais apraksts; un visbeidzot 4) apstrādes darbību atbalstošā IT infrastruktūra, tostarp operētājsistēmas, virtuālās sistēmas, datu bāzes, autentifikācijas un autorizācijas sistēmas, maršrutētāji un ugunsmūri, uzglabāšanas sistēmas, sakaru infrastruktūra vai piekļuve internetam, kā arī saistītie tehniskie pasākumi.

53. Visi trīs galvenie komponenti ir būtiski sertifikācijas procedūru un kritēriju izstrādē. Atkarībā no sertifikācijas objekta var atšķirties tas, cik lielā mērā tie tiek ņemti vērā. Piemēram, dažos gadījumos dažus komponentus var neņemt vērā, ja tie tiek uzskatīti par sertifikācijas objektam nebūtiskiem.

54. Lai precizētu, ko var sertificēt saskaņā ar VDAR, VDAR sniegti papildu norādījumi. No 42. panta 7. punkta izriet, ka sertifikātus saskaņā ar VDAR izsniedz tikai datu pārziņiem un datu apstrādātājiem, izslēdzot, piemēram, datu aizsardzības speciālistu sertifikāciju. 43. panta 1. punkta b) apakšpunkts atsaucas uz ISO 17065, kurā paredzēta sertifikācijas struktūru akreditācija, kas novērtē produktu, pakalpojumu un procesu atbilstību. Apstrādes darbība vai darbību kopums var radīt produktu vai pakalpojumu atbilstīgi ISO 17065 terminoloģijai, un to var sertificēt. Piemēram, darbinieku datu apstrāde algas vai atvaļinājuma pārvaldības nolūkā ir darbību kopums VDAR izpratnē un var radīt produkta, procesa vai pakalpojuma sniegšanu atbilstīgi ISO terminoloģijai.

55. Pamatojoties uz šiem apsvērumiem, EDAK uzskata, ka sertifikācijas piemērošanas joma saskaņā ar VDAR ir vērsta uz apstrādes darbībām vai darbību kopumiem. Tie var ietvert pārvaldības procesus organizatorisku pasākumu izpratnē, tātad kā apstrādes procesa neatņemamu sastāvdaļu (piemēram, vadības process, kas noteikts sūdzību izskatīšanai darbinieku datu apstrādes ietvaros algu maksāšanas nolūkā).

56. Lai novērtētu apstrādes darbības atbilstību sertifikācijas kritērijiem, jānorāda lietošanas gadījums. Piemēram, apstrādes darbībā izmantotās tehniskās infrastruktūras izmantošanas atbilstība ir atkarīga no datu kategorijām, kuras tai paredzēts apstrādāt. Organizatoriskie pasākumi ir atkarīgi no datu kategorijām un apjoma, kā arī apstrādei izmantotās tehniskās infrastruktūras, ņemot vērā apstrādes raksturu, apjomu, saturu un mērķus, kā arī riskus datu subjektu tiesībām un brīvībām.

57. Turklāt jāpatur prātā, ka IT lietojumprogrammas var būt ļoti atšķirīgas, lai arī tās kalpo vienādiem apstrādes nolūkiem. Tādēļ tas ir jāņem vērā, nosakot sertifikācijas mehānismu piemērošanas jomu un izstrādājot sertifikācijas kritērijus, t. i., sertifikācijas un kritēriju piemērošanas jomai nevajadzētu būt tik šaurai, lai izslēgtu atšķirīgas IT lietojumprogrammas.

## 5.2 Sertifikācijas objekta noteikšana

58. Sertifikācijas mehānisma piemērošanas joma ir jānošķir no objekta, ko sauc arī par novērtēšanas mērķi (ToE), atsevišķos sertifikācijas projektos saskaņā ar sertifikācijas mehānismu. Sertifikācijas mehānisms var definēt savu piemērošanas jomu vispārīgi vai saistībā ar konkrētu apstrādes darbību veidu vai jomu, un tādējādi tas jau var noteikt sertifikācijas objektus, kuri ietilpst sertifikācijas mehānisma piemērošanas jomā (piemēram,

droša glabāšana un digitālajā glabātuvē uzglabāto personas datu aizsardzība). Jebkurā gadījumā uzticamu un jēgpilnu atbilstības novērtējumu var veikt tikai tad, ja ir precīzi aprakstīts sertifikācijas projekta atsevišķais objekts. Skaidri jāapraksta, kuras apstrādes darbības ir iekļautas sertifikācijas objektā, un pēc tam galvenos komponentus, t. i., kādi dati, procesi un tehniskā infrastruktūra tiks novērtēti un kādi ne. To darot, vienmēr ir jāņem vērā un jāapraksta saskarnes ar citiem procesiem. Saprotams, novērtējumā nevar iekļaut to, kas nav zināms, un tādējādi to nevar sertificēt. Jebkurā gadījumā atsevišķam sertifikācijas objektam ir jābūt nozīmīgam attiecībā uz ziņojumu vai prasījumu, kas veikts sertifikācijā, un tam nevajadzētu maldināt lietotāju, klientu vai patērētāju.

59. [1. piemērs]

Banka saviem klientiem piedāvā tīmekļa vietni internetbankas pakalpojumiem. Šī pakalpojuma ietvaros ir iespējams veikt pārskaitījumus, iegādāties kapitāldaļas, uzsākt pastāvīgus maksājumus un pārvaldīt kontu. Banka vēlas sertificēt šādu informāciju atbilstīgi datu aizsardzības sertifikācijas mehānismam ar vispārēju piemērošanas jomu, pamatojoties uz vispārējiem kritērijiem:

a) Droša pieteikšanās

Droša pieteikšanās ir apstrādes darbība, kas ir saprotama gala lietotājam un kas ir svarīga no datu aizsardzības viedokļa, jo tai ir būtiska loma iesaistīto personas datu drošības nodrošināšanā. Tādēļ šī apstrādes darbība ir nepieciešama drošas pieteikšanās nodrošināšanai un tā var būt nozīmīgs ToE, ja sertifikātā ir skaidri norādīts, ka sertificēta ir tikai pieteikšanās apstrādes darbība.

b) Tīmekļa priekšgals

Lai gan tīmekļa priekšgals var būt svarīgs no datu aizsardzības viedokļa, tas nav saprotams gala lietotājam, un tāpēc tas nevar būt nozīmīgs ToE. Turklāt lietotājam nav skaidrs, kādi pakalpojumi tīmekļa vietnē un tādējādi kuras apstrādes darbības ir sertificēti.

c) Internetbankas pakalpojumi

Tīmekļa priekšgals kopā ar aizmugursistēmu ir apstrādes darbības, kuras tiek sniegtas internetbankas pakalpojumu ietvaros, kas var būt nozīmīgas lietotājam. Šajā kontekstā abi ir ietverti ToE. Savukārt apstrādes darbības, kas nav tieši saistītas ar internetbankas pakalpojumu sniegšanu, piemēram, apstrādes darbības nelikumīgi iegūtu līdzekļu legalizācijas novēršanai, var izslēgt no ToE.

Tomēr internetbankas pakalpojumi, ko banka piedāvā savā tīmekļa vietnē, var ietvert arī citus pakalpojumus, kam savukārt nepieciešamas savas apstrādes darbības. Šajā sakarā citi pakalpojumi var ietvert, piemēram, apdrošināšanas produkta piedāvāšanu. Tā kā šis papildu pakalpojums nav tieši saistīts ar internetbankas pakalpojumu sniegšanas nolūku, to var izslēgt no ToE. Ja šis papildu pakalpojums (apdrošināšana) tiek izslēgts no ToE, šī pakalpojuma saskarnes, kas integrētas tīmekļa vietnē, ietilpst ToE, un tādēļ tās ir jāapraksta, lai skaidri nodalītu pakalpojumus. Šāds apraksts ir nepieciešams, lai noteiktu un izvērtētu iespējamās datu plūsmas starp abiem pakalpojumiem.

60. [2. piemērs]

Banka saviem klientiem piedāvā pakalpojumu, kas ļauj apkopot ar dažādiem kontiem un kredītkartēm no vairākām bankām saistītu informāciju (kontu apkopošana). Banka vēlas sertificēt savus pakalpojumus saskaņā ar VDAR. Kompetentā uzraudzības iestāde ir apstiprinājusi īpašu sertifikācijas kritēriju kopumu šāda veida darbībai. Sertifikācijas mehānisma piemērošanas joma attiecas tikai uz šādiem atbilstības aspektiem:

- lietotāja autentifikācija; un
- pieņemams veids, kādā iegūt apkopojamos datus no citām bankām/pakalpojumiem.

Tā kā šī sertifikācijas mehānisma piemērošanas joma pati par sevi definē ToE, nav iespējams jēgpilni sašaurināt ToE saskaņā ar ierosināto piemērošanas jomu un sertificēt tikai konkrētas iezīmes vai vienu apstrādes darbību. Šajā gadījumā ToE ir jāsakrīt ar konkrēto piemērošanas jomu.

## 5.3 Izvērtēšanas metodes un novērtēšanas metodika

61. Lai palīdzētu uzskatāmi parādīt apstrādes darbību atbilstību, atbilstības novērtējumā ir jāidentificē un jānosaka izvērtēšanas metodes un novērtēšanas metodika. Ir svarīgi, vai novērtējumam nepieciešamā informācija tiek vākta tikai no dokumentācijas (kas pati par sevi nebūtu pietiekama) vai arī tā tiek aktīvi vākta uz vietas, kā arī izmantojot tiešu vai netiešu piekļuvi. Informācijas vākšanas veids ietekmē sertifikācijas nozīmīgumu, un tādēļ tas būtu jādefinē un jāapraksta.

    Sertifikātu izsniegšanas un periodiskās pārskatīšanas procedūrās jāiekļauj specifikācijas, ar ko nosaka piemēroto izvērtēšanas līmeni (dziļumu un detalizāciju), lai izpildītu sertifikācijas kritērijus, un tajā būtu jāiekļauj:

    - informācija par piemērojamajām novērtēšanas metodēm un to specifikācija, kā arī, piemēram, konstatējumi, kas iegūti, veicot revīzijas uz vietas vai izskatot dokumentāciju,
    - izvērtēšanas metodes, kurās galvenā uzmanība pievērsta apstrādes darbībām (dati, sistēmas, procesi) un apstrādes nolūkam,
    - datu kategoriju noteikšana, aizsardzības vajadzības, kā arī tas, vai ir iesaistīti apstrādātāji vai trešās personas,
    - funkciju noteikšana un attiecībā uz funkcijām un pienākumiem definēta piekļuves kontroles mehānisma esība.

62. Izvērtējuma dziļums ietekmē sertifikācijas nozīmīgumu un vērtību. Samazinot izvērtējuma dziļumu pragmatiskiem nolūkiem vai samazinot izmaksas, tiks samazināta datu aizsardzības sertifikācijas nozīme. No otras puses, lēmumi par izvērtējuma detalizētību var pārsniegt pieteikuma iesniedzēja finansiālās iespējas un bieži vien arī vērtētāju un revidentu spējas. Atbilstības uzskatāmas parādīšanas nolūkos ne vienmēr ir nepieciešams veikt ļoti detalizētu IT sistēmu analīzi, lai novērtējums būtu jēgpilns.

## 5.4 Novērtējuma dokumentācija

63. Sertifikācijas dokumentācijai vajadzētu būt pilnīgai un visaptverošai. Iztrūkstot dokumentācijai, nav iespējams veikt pareizu novērtējumu. Sertifikācijas dokumentācijas pamatfunkcija ir nodrošināt pārredzamību izvērtēšanas procesā saskaņā ar sertifikācijas mehānismu. Dokumentācijā sniedz atbildes uz jautājumiem par likumā noteiktajām prasībām. Sertifikācijas mehānismiem būtu jāparedz standartizēta dokumentācijas metodika. Pēc tam izvērtēšana ļaus salīdzināt sertifikācijas dokumentus ar faktisko statusu uz vietas un sertifikācijas kritērijiem.

64. Visaptveroša dokumentācija par to, kas ticis sertificēts, un izmantoto metodiku kalpo pārredzamībai. Saskaņā ar 43. panta 2. punkta c) apakšpunktu sertifikācijas mehānismiem būtu jāizstrādā procedūras, kas ļauj pārskatīt sertifikātus. Lai uzraudzības iestāde varētu novērtēt, vai un cik lielā mērā sertifikāciju var atzīt oficiālās izmeklēšanās, detalizētāka dokumentācija var būt vispiemērotākais informēšanas veids. Tādēļ izvērtēšanas laikā sagatavotajā dokumentācijā būtu jākoncentrējas uz trim galvenajiem aspektiem:

- izmantoto izvērtēšanas metožu konsekvenci un saskaņotību;
- izvērtēšanas metodēm, kas vērstas uz to, lai uzskatāmi parādītu sertifikācijas objekta atbilstību sertifikācijas kritērijiem un līdz ar to regulai; un
- faktu, ka izvērtēšanas rezultātus ir apstiprinājusi neatkarīga un objektīva sertifikācijas struktūra.

## 5.5 Rezultātu dokumentēšana

65. VDAR 100. apsvērumā sniegta informācija par sertifikācijas ieviešanas mērķiem.

“Lai uzlabotu pārredzamību un šīs regulas ievērošanu, būtu jāiedrošina izstrādāt sertifikācijas mehānismus un datu aizsardzības zīmogus un marķējumus, kas ļautu datu subjektam ātri novērtēt datu aizsardzības līmeni saistībā ar konkrētiem produktiem un pakalpojumiem.”

66. Rezultātu dokumentēšanai un izziņošanai ir būtiska loma pārredzamības uzlabošanā. Sertifikācijas struktūrām, kuras izmanto uz datu subjektiem (kā patērētājiem vai klientiem) vērstus sertifikācijas mehānismus, zīmogus vai marķējumus, būtu jāsniedz viegli pieejama, saprotama un jēgpilna informācija par sertificēto(-ajām) apstrādes darbību(-ām). Šajā publiski pieejamajā informācijā būtu jāiekļauj vismaz:

- ToE apraksts;
- atsauce uz apstiprinātajiem kritērijiem, kas piemēroti konkrētam ToE;
- kritēriju izvērtēšanas metodika (izvērtēšana uz vietas, dokumentācija utt.); un
- sertifikāta derīguma termiņš; un
- tai būtu jānodrošina rezultātu salīdzināmība uzraudzības iestādēm un sabiedrībai.

# 6 NORĀDĪJUMI SERTIFIKĀCIJAS KRITĒRIJU DEFINĒŠANAI

67. Sertifikācijas kritēriji ir neatņemama sertifikācijas mehānisma sastāvdaļa. Sertifikācijas procedūra ietver prasības par to, kā, kurš, cik lielā mērā un cik detalizēti veic novērtējumu atsevišķos sertifikācijas projektos attiecībā uz konkrētu objektu vai novērtēšanas mērķi (ToE). Sertifikācijas kritērijos noteiktas nominālās prasības, novērtējot faktisko apstrādes darbību, kas noteikta ToE. Šajās pamatnostādnēs sertifikācijas kritēriju noteikšanai sniegti vispārīgi padomi, kas atvieglos sertifikācijas kritēriju novērtēšanu apstiprināšanas nolūkā.

    - Apstiprinot vai nosakot sertificēšanas kritērijus, būtu jāņem vērā šādi vispārīgi apsvērumi. Sertificēšanas kritērijiem vajadzētu būt:
    - vienādiem un pārbaudāmiem;
    - revidējamiem, lai atvieglotu apstrādes darbību izvērtēšanu saskaņā ar VDAR, jo īpaši norādot mērķus un īstenošanas norādījumus šo mērķu sasniegšanai;
    - jāattiecas uz mērķauditoriju (piemēram, B2B jeb uzņēmums uzņēmumam vai B2C jeb uzņēmums klientam);
    - jāņem vērā un attiecīgā gadījumā jābūt savstarpēji savietojamiem ar citiem standartiem (piemēram, ISO standartiem, valsts līmeņa standartiem); un
    - jābūt elastīgiem un pielāgojamiem, lai tos varētu piemērot dažādiem organizāciju veidiem un izmēriem, tostarp mikrouzņēmumiem, maziem un vidējiem uzņēmumiem saskaņā ar 42. panta 1. punktu, un uz risku balstītai pieejai saskaņā ar 77. apsvērumu.

68. Mazs vietējais uzņēmums, piemēram, mazumtirgotājs, parasti veic mazāk sarežģītas apstrādes darbības nekā liels starptautisks mazumtirgotājs. Lai gan apstrādes darbību likumības prasības ir vienādas, jāņem vērā datu apstrādes apjoms un sarežģītība; no tā izriet, ka sertifikācijas mehānismi un to kritēriji ir pielāgojami atbilstoši attiecīgajai apstrādes darbībai.

## 6.1 Spēkā esošie standarti

69. Sertifikācijas struktūrām būs jāapsver, kā konkrētos kritērijos ņemti vērā spēkā esošie attiecīgie instrumenti, piemēram, rīcības kodeksi, tehniskie standarti vai valstu normatīvās un juridiskās iniciatīvas. Ideālā gadījumā kritēriji būs savstarpēji savietojami ar spēkā esošajiem standartiem, kas var palīdzēt pārzinim vai apstrādātājam izpildīt savus VDAR paredzētos pienākumus. Tomēr, lai gan nozares standarti bieži vien ir vērsti uz organizācijas aizsardzību un drošību pret apdraudējumu, VDAR ir vērsta uz fizisko personu pamattiesību aizsardzību. Šī atšķirīgā perspektīva ir jāņem vērā, izstrādājot kritērijus vai apstiprinot kritērijus vai sertifikācijas mehānismus, kuru pamatā ir nozares standarti.

## 6.2 Kritēriju definēšana

70. Sertifikācijas kritērijiem jāatbilst sertifikācijas mehānisma vai sistēmas sertifikācijas paziņojumam (ziņojumam vai prasījumam) un jāatbilst tā izvirzītajām cerībām. Sertifikācijas mehānisma nosaukumā jau var identificēt piemērošanas jomu, un tas ietekmēs kritēriju noteikšanu.

71. [3. piemērs]

    Mehānisma, ko sauc par "HealthPrivacyMark", piemērošanas jomai vajadzētu būt attiecināmai tikai uz veselības aprūpes nozari. Zīmoga nosaukums liek sagaidīt, ka tiks pārbaudītas datu aizsardzības prasības saistībā ar veselības datiem. Attiecīgi šī mehānisma kritērijiem jābūt atbilstošiem, lai novērtētu datu aizsardzības prasības šajā nozarē.

72. [4. piemērs]

    Mehānismam, kas attiecas uz tādu apstrādes darbību sertificēšanu, kuras ietver datu apstrādes pārvaldības sistēmas, būtu jānosaka kritēriji, kas ļauj atzīt un novērtēt pārvaldības procesus un to tehniskos un organizatoriskos atbalsta pasākumus.

73. [5. piemērs]

    Kritērijos mehānismam, kas attiecas uz mākoņdatošanu, jāņem vērā īpašas tehniskās prasības, kas nepieciešamas mākonī balstītu pakalpojumu izmantošanai. Piemēram, ja serveri tiek izmantoti ārpus ES, kritērijos jāņem vērā VDAR V nodaļā izklāstītie nosacījumi attiecībā uz datu nosūtīšanu trešām valstīm.

74. Kritērijiem, kas paredzēti, lai dažādās nozarēs un/vai dalībvalstīs piemērotu dažādus ToE, vajadzētu: ļaut piemērot dažādus scenārijus; ļaut noteikt piemērotus pasākumus, kas atbilst maza, vidēja vai liela mēroga apstrādes darbībām un atspoguļo risku fizisku personu tiesībām un brīvībām — ar atšķirīgu iespējamību un nopietnību — atbilstīgi VDAR. Tādējādi sertifikācijas procedūrām (piemēram, dokumentācijai, testēšanai vai izvērtēšanas metodei un dziļumam), ar ko papildina kritērijus, jāatbilst šīm vajadzībām un jāļauj un jāievieš noteikumi, lai, piemēram, piemērotu attiecīgos kritērijus atsevišķos sertifikācijas projektos. Kritērijiem jāļauj vieglāk novērtēt, vai ir sniegtas pietiekamas garantijas atbilstošu tehnisku un organizatorisku pasākumu īstenošanai.

## 6.3 Sertifikācijas kritēriju kalpošanas ilgums

75. Lai gan sertifikācijas kritērijiem ir jābūt uzticamiem ilgākā laika periodā, tie nedrīkst būt akmenī kalti. Tos pārskata, piemēram, ja:

    - tiek grozīts tiesiskais regulējums;
    - Eiropas Savienības tiesas spriedumos ir interpretēti termini un noteikumi; vai
    - tehnoloģiju līmenis ir attīstījies.

Priekšsēdētājs

(*Andrea Jelinek*)



pieņemts

# 1. PIELIKUMS. UZRAUDZĪBAS IESTĀŽU UZDEVUMI UN PILNVARAS ATTIECĪBĀ UZ SERTIFIKĀCIJU SASKAŅĀ AR VDAR

| | Noteikumi | Prasības |
|---|---|---|
| **Uzdevumi** | 43. panta 6. punkts | Pieprasa uzraudzības iestādei publiskot 42. panta 5. punktā minētos kritērijus viegli pieejamā veidā un nosūtīt tos kolēģijai. |
| | 57. panta 1. punkta n) apakšpunkts | Pieprasa uzraudzības iestādei apstiprināt sertifikācijas kritērijus saskaņā ar 42. panta 5. punktu. |
| | 57. panta 1. punkta o) apakšpunkts | Nodrošina, ka attiecīgā gadījumā (t. i., izdodot sertifikātu) tā periodiski pārskata izdoto sertifikātu saskaņā ar 42. panta 7. punktu. |
| | 64. panta 1. punkta c) apakšpunkts | Pieprasa uzraudzības iestādei informēt kolēģiju par lēmuma projektu, ja tā vēlas apstiprināt 42. panta 5. punktā minētos sertifikācijas kritērijus. |
| **Pilnvaras** | 58. panta 1. punkta c) apakšpunkts | Piešķir uzraudzības iestādei pilnvaras veikt sertifikācijas pārskatīšanu saskaņā ar 42. panta 7. punktu. |
| | 58. panta 2. punkta h) apakšpunkts | Paredz uzraudzības iestādei pilnvaras atsaukt vai uzdot sertifikācijas struktūrai atsaukt sertifikātu vai uzdot sertifikācijas struktūrai neizdot sertifikātu. |
| | 58. panta 3. punkta e) apakšpunkts | Paredz uzraudzības iestādei pilnvaras akreditēt sertifikācijas struktūras. |
| | 58. panta 3. punkta f) apakšpunkts | Paredz uzraudzības iestādei pilnvaras izdot sertifikātus un apstiprināt sertificēšanas kritērijus. |
| | 58. panta 3. punkta e) apakšpunkts | Paredz uzraudzības iestādei pilnvaras akreditēt sertifikācijas struktūras. |
| | 58. panta 3. punkta f) apakšpunkts | Paredz uzraudzības iestādei pilnvaras izdot sertifikātus un apstiprināt sertificēšanas kritērijus. |

# 2. PIELIKUMS

## 1 IEVADS

2. pielikumā sniegtas norādes sertifikācijas kritēriju pārskatīšanai un novērtēšanai saskaņā ar 42. panta 5. punktu. Tajā identificētas tēmas, kuras datu aizsardzības uzraudzības iestāde un EDAK apsvērs un piemēros sertifikācijas mehānisma sertifikācijas kritēriju apstiprināšanas nolūkā. Jautājumi ir jāizskata sertifikācijas struktūrām un sistēmu īpašniekiem, kuri vēlas izstrādāt un iesniegt kritērijus apstiprināšanai. Saraksts nav izsmeļošs, taču tajā uzskaitīts minimālais apskatāmo tēmu saraksts. Ne visi jautājumi būs piemērojami; tomēr tie būtu jāņem vērā, izstrādājot kritērijus, un var būt nepieciešams argumentēti izskaidrot, kādēļ kritēriji neaptver konkrētus aspektus. Daži jautājumi atkārtojas, jo uzdoti no atšķirīga viedokļa. Šīs norādes būtu jāizskata saskaņā ar VDAR un attiecīgos gadījumos valsts tiesību aktos sniegtajām juridiskajām prasībām.

## 2 SERTIFIKĀCIJAS MEHĀNISMA UN NOVĒRTĒŠANAS MĒRĶA (TOE) TVĒRUMS

a. Vai sertifikācijas mehānisma (kuram izmanto datu aizsardzības kritērijus) piemērošanas joma ir skaidri aprakstīta?

b. Vai sertifikācijas mehānisma piemērošanas jomas nozīme ir saprotama paredzētajai mērķauditorijai un nav maldinoša?

- *Piemēram: "Uzticama uzņēmuma zīmogs" rosina domāt, ka visām uzņēmuma apstrādes darbībām ir veikts audits, kaut arī tikai noteiktas apstrādes darbības, piem. tiešsaistes maksājumu process, ir faktiski sertificētas. Piemērošanas joma līdz ar to ir maldinoša.*

c. Vai sertifikācijas mehānisma piemērošanas jomā atspoguļoti visi apstrādes darbību būtiskie aspekti?

- *Piemēram: "Privātuma veselības marķējumā" ir jāiekļauj visi izvērtējamie veselības dati, lai nodrošinātu atbilstību 9. pantā noteiktajām prasībām.*

d. Vai sertifikācijas mehānisma piemērošanas joma ļauj veikt jēgpilnu datu aizsardzības sertifikāciju, ņemot vērā saistīto apstrādes darbību būtību, saturu un risku?

- *Piemēram: Ja sertifikācijas mehānisma piemērošanas joma ir vērsta tikai uz apstrādes darbību konkrētiem aspektiem, piemēram, datu vākšanu, taču ne turpmākajām apstrādes darbībām, piemēram, apstrādi reklāmas profilu izveides nolūkā vai datu subjekta tiesību pārvaldības nolūkā, tas nebūs jēgpilni datu subjektiem.*

e. Vai sertifikācijas mehānisma piemērošanas joma aptver personas datu apstrādi attiecīgajā piemērošanas valstī un vai tas skar datu pārrobežu apstrādi un/vai nosūtīšanu?

f. Vai sertifikācijas kritērijos pietiekamā apmērā aprakstīts, kā definēt ToE?

- *Piemēram: "Privātuma zīmogs" ar vispārēju tvērumu, pieprasot tikai "sertifikācijai pakļautas apstrādes precizēšanu", nesniegtu pietiekami skaidru norādījumu par to, kā noteikt un aprakstīt ToE.*
- *Piemēram: (Konkrētas) piemērošanas jomas, "Privātuma seifa zīmogs", kas vērsta uz drošu uzglabāšanu, kritērijos būtu sīki jāapraksta prasības atbilstības tvēruma*

*nodrošināšanai, piemēram, glabātuves definīcija, sistēmas prasības, obligātie tehniskie un organizatoriskie pasākumi (TOM). Šādā gadījumā piemērošanas jomā var skaidri definēt ToE.*

(1) Vai kritēriji paredz ToE iekļaut visu būtisko apstrādes darbību identifikāciju, datplūsmas ilustrāciju un ToE piemērošanas jomas noteikšanu?

- *Piemēram: Sertifikācijas mehānismā piedāvāta datu pārziņu apstrādes darbību sertifikācija saskaņā ar VDAR, neprecizējot piemērošanas jomu (vispārīgs tvērums). Mehānismā izmantotie kritēriji paredz pieteikuma iesniedzējam datu pārzinim noteikt mērķtiecīgu apstrādes darbību (ToE) attiecībā uz izmantotajiem datu veidiem, sistēmām un procesiem.*

(2) Vai kritēriji paredz pieteikuma iesniedzējam precizēt, kur sākas un beidzas novērtējumam pakļautā apstrāde? Vai kritēriji paredz ToE iekļaut saskarnes gadījumos, kad neatkarīgas apstrādes darbības nav iekļautas ToE ietvaros? Un vai tas ir pietiekami pamatots?

- *Piemēram: ToE, kur pietiekami detalizēti aprakstīta tīmeklī balstīta pakalpojuma apstrādes darbība, piemēram, lietotāju reģistrēšana, pakalpojumu sniegšana, rēķinu izstādīšana, IP adrešu reģistrēšana, saskarnes lietotājiem un trešām personām un izņemot servera mitināšanu (tomēr ietverot apstrādi un TOM nolīgumus).*

g. Vai kritēriji garantē to, ka (atsevišķi) ToE ir saprotami to mērķauditorijai, tostarp attiecīgos gadījumos datu subjektiem?

# 3 VISPĀRĪGAS PRASĪBAS

a. Vai visi kritēriju katalogā (t. i., pilns sertifikācijas kritēriju kopums) izmantotie būtiskie termini ir identificēti, paskaidroti un aprakstīti?

b. Vai ir identificētas normatīvās atsauces?

c. Vai kritērijos ietverta datu aizsardzības pienākumu, procedūru un procesu, kas ietilpst sertifikācijas mehānisma piemērošanas jomā, definīcija?

# 4 APSTRĀDES DARBĪBA, 42. PANTA 1. PUNKTS

Attiecībā uz sertifikācijas mehānisma piemērošanas jomu (vispārīgs vai konkrēts) — vai kritērijos ir aplūkoti visi apstrādes darbību būtiskie komponenti (dati, sistēmas un procesi)?

a. Vai kritēriji paredz spēkā esoša apstrādes juridiskā pamata norādīšanu attiecībā uz ToE?

b. Vai attiecībā uz ToE kritērijos atzītas būtiskās apstrādes fāzes un pilns datu dzīves cikls, tostarp dzēšana un anonimizācija?

c. Vai attiecībā uz ToE kritēriji paredz datu pārnesamību?

d. Vai attiecībā uz ToE kritēriji ļauj identificēt un atspoguļot īpašus apstrādes darbību veidus, piemēram, automatizētu lēmumu pieņemšanu, profilēšanu?

e. Vai attiecībā uz ToE kritēriji ļauj identificēt īpašas datu kategorijas?

f. Vai kritēriji ļauj un paredz novērtēt atsevišķu apstrādes darbību risku un datu subjektu tiesību un brīvību aizsardzības vajadzības?

g. Vai kritēriji ļauj un paredz veikt atbilstošu fizisku personu tiesību un brīvību risku uzskaiti?

(…)

# 5 APSTRĀDES LIKUMĪGUMS

a. Vai kritēriji paredz pārbaudīt atsevišķu apstrādes darbību likumīgumu attiecībā uz apstrādes nolūkiem un nepieciešamību?

b. Vai kritēriji paredz pārbaudīt visas atsevišķu apstrādes darbību juridiskā pamata prasības?

# 6 PRINCIPI, 5. PANTS

a. Vai kritērijos pienācīgi aplūkoti visi datu aizsardzības principi atbilstīgi 5. pantam?

b. Vai kritēriji paredz datu minimizācijas apliecināšanu atsevišķiem ToE?

(…)

# 7 VISPĀRĪGI DATU PĀRZIŅU UN APSTRĀDĀTĀJU PIENĀKUMI

a. Vai kritēriji paredz uzrādīt līgumiskas vienošanās starp apstrādātājiem un pārziņiem pierādījumus?

b. Vai pārziņu un apstrādātāju vienošanās tiek izvērtētas?

c. Vai kritērijos ir atspoguļoti pārziņa pienākumi saskaņā ar IV nodaļu?

d. Vai kritēriji paredz pierādīt pārziņa atbilstīgi 24. panta 1. punktam īstenoto tehnisko un organizatorisko pasākumu pārskatīšanu un atjaunināšanu?

e. Vai kritēriji pārbauda, vai organizācija ir novērtējusi Datu aizsardzības speciālista (DAS) iecelšanas nepieciešamību atbilstīgi 37. pantam? Attiecīgos gadījumos — vai DAS atbilst 37. un 39. pantā noteiktajām prasībām?

f. Vai kritēriji pārbauda, vai saskaņā ar 30. panta 5. punktu ir jāveic ieraksti par apstrādes darbībām un vai ir pienācīgi aplūkotas 30. pantā ietvertās prasības?

# 8 DATU SUBJEKTU TIESĪBAS

a. Vai kritērijos pietiekami risinātas datu subjekta tiesības uz informāciju un paredzēta attiecīgo pasākumu ieviešana?

b. Vai kritēriji paredz datu subjektiem piešķirt pienācīgu vai pat lielāku piekļuvi viņu datiem un kontroli pār tiem, tostarp datu pārnesamību?

c. Vai kritēriji paredz ieviest pasākumus, kas nodrošina iespēju iejaukties apstrādes darbībā, lai garantētu datu subjektu tiesības, kā arī ļautu veikt labojumus, dzēst un ierobežot?

(…)

# 9 FIZISKU PERSONU TIESĪBU UN BRĪVĪBU RISKI

a. Vai kritēriji ļauj un paredz novērtēt fizisku personu tiesību un brīvību riskus?

b. Vai kritēriji sniedz vai paredz atzītu riska novērtēšanas metodiku? Attiecīgā gadījumā — vai tā ir samērīga?

c. Vai kritēriji ļauj un paredz novērtēt paredzamo apstrādes darbību ietekmi uz fizisku personu tiesībām un brīvībām?

d. Vai kritēriji paredz iepriekšēju apspriešanos par pārējiem riskiem, kurus nav iespējams mazināt, balstoties uz Datu aizsardzības ietekmes novērtējuma (DAIN) rezultātiem?

# 10 TEHNISKI UN ORGANIZATORISKI PASĀKUMI, AR KO GARANTĒ AIZSARDZĪBU

a. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu apstrādes darbību konfidencialitātes nodrošināšanai?

b. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu apstrādes darbību integritātes nodrošināšanai?

c. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu apstrādes darbību pieejamības nodrošināšanai?

d. Vai kritēriji paredz pasākumu piemērošanu, ar ko nodrošina apstrādes darbību pārredzamību attiecībā uz

e. pārskatatbildību?

f. datu subjektu tiesībām?

g. atsevišķu apstrādes darbību novērtēšanu, piemēram, algoritmu pārredzamībai?

h. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu datu subjekta tiesību garantēšanai, piemēram, spēja sniegt informāciju vai datu pārnesamība?

i. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu, kas nodrošina iespēju iejaukties apstrādes darbībā, lai garantētu datu subjekta tiesības, kā arī ļautu veikt labojumus, dzēst un ierobežot?

j. Vai kritēriji paredz piemērot pasākumus, kas nodrošina iespēju iejaukties apstrādes darbībā, lai garantētu datu subjekta tiesības, lai labotu vai pārbaudītu sistēmu vai procesu?

k. Vai kritēriji paredz tehnisku un organizatorisku pasākumu piemērošanu, lai nodrošinātu datu minimizāciju, piemēram, datu atvienošanu vai atdalīšanu no datu subjekta, anonimizāciju vai pseidonimizāciju, vai datu sistēmu izolāciju?

l. Vai kritēriji paredz pēc noklusējuma ieviest tehniskus pasākumus datu aizsardzības īstenošanai?

m. Vai kritēriji paredz tehniskus un organizatoriskus pasākumus integrētas datu aizsardzības ieviešanai, piemēram, datu aizsardzības pārvaldības sistēmu, kas parāda, informē, kontrolē un izpilda datu aizsardzības prasības?

n. Vai kritēriji paredz tehniskus un organizatoriskus pasākumus, ar ko īsteno darbinieku, kuriem ir pastāvīga vai regulāra piekļuve personas datiem, atbilstošu periodisku apmācību un izglītošanu?

o. Vai kritēriji paredz pasākumu pārskatīšanu?

p. Vai kritēriji paredz pašnovērtējumu / iekšējo auditu?

q. Vai kritēriji paredz pasākumu, ar ko nodrošina, ka ziņošanas par personas datu aizsardzības pārkāpumu pienākums tiek izpildīts attiecīgajā laikā un apmērā?

r. Vai kritēriji paredz ieviest un pārbaudīt drošības pārkāpuma pārvaldības procedūras?

s. Vai kritēriji paredz nepārtraukti attīstošo privātuma un tehnoloģiju jautājumu uzraudzību un sistēmas atjauninašanu nepieciešamības gadījumā?

(…)

# 11 CITAS ĪPAŠAS DATU AIZSARDZĪBAI DRAUDZĪGAS IESPĒJAS

a. Vai kritēriji paredz datu aizsardzību uzlabojošu tehnoloģiju ieviešanu? Šeit varētu būt ietverti kritēriji, kas pieprasa uzlabotu datu aizsardzību, novēršot vai samazinot personas datu un/vai datu aizsardzības risku.

- *Piemēram: Kritēriji, kas prasa uzlabotu atvienošanas iespēju, izmantojot uz lietotāju orientētu identitātes pārvaldību, piemēram, uz atribūtiem balstīti akreditācijas dati (ABC), nevis uz organizāciju vērstu identitātes pārvaldību, atspoguļotu datu aizsardzības uzlabošanas tehniku.*

b. Vai kritēriji paredz uzlabotas datu subjektu kontroles īstenošanu nolūkā atvieglot neatkarību un izvēli?

(…)

# 12 KRITĒRIJI, KURU NOLŪKS IR PIERĀDĪT, KA PASTĀV PIENĀCĪGI AIZSARDZĪBAS PASĀKUMI PERSONAS DATU NOSŪTĪŠANAI

Šie kritēriji tiks aplūkoti turpmākajās pamatnostādnēs par 42. panta 2. punktu.

# 13 PAPILDU KRITĒRIJI EIROPAS DATU AIZSARDZĪBAS ZĪMOGAM

a. Vai kritēriji paredz aptvert visas dalībvalstis?

b. Vai kritēriji spēj ņemt vērā dalībvalsts datu aizsardzības tiesību aktus vai scenārijus?

c. Vai kritēriji paredz atsevišķu ToE izvērtēšanu attiecībā uz dalībvalsts datu aizsardzības tiesību aktiem konkrētai nozarei?

d. Vai kritēriji paredz pārzinim vai apstrādātājam sniegt informāciju datu subjektiem un ieinteresētajām personām dalībvalsts valodās par

e. apstrādi/ToE?

f. apstrādes dokumentēšanu/ToE?

g. izvērtēšanas rezultātiem?

(…)

# 14 VISPĀRĒJĀ KRITĒRIJU IZVĒRTĒŠANA

a. Vai kritēriji pilnībā aptver sertifikācijas mehānisma piemērošanas jomu (t. i., vispārīgie kritēriji), lai sniegtu pietiekamas garantijas un nodrošinātu sertifikācijas uzticamību?

- *Piemēram: Ja sertifikācijas mehānisma piemērošanas joma galvenokārt vērsta uz veselības datu apstrādes darbībām, ir jāgarantē augsta līmeņa datu aizsardzība, definējot kritērijus, kas nodrošina, piemēram, padziļinātu novērtējumu un privātuma aizsardzības pēc noklusējuma un integrēta privātuma aizsardzības principu piemērošanu.*

b. Vai kritēriji ir samērīgi ar tās apstrādes darbības apmēru, uz kuru attiecas sertifikācijas mehānisma piemērošanas joma, informācijas sensitivitāte un apstrādes risks?

c. Vai ir ticams, ka kritēriji uzlabos pārziņu un apstrādātāju atbilstību datu aizsardzības prasībām?

d. Vai datu subjekti būs ieguvēji attiecībā uz viņu tiesībām uz informāciju, tostarp, paskaidrojot datu subjektiem vēlamo iznākumu?