



Sertifikācijas institūcijas (struktūras) akreditācijas prasības

Priekšvārds

Šajā dokumentā Datu valsts inspekcija (turpmāk — Inspekcija) saskaņā ar Vispārīgās datu aizsardzības regulas (turpmāk — Datu regula) 43. panta 2. punktu, 58. panta 3. punkta e) un f) apakšpunktu¹, Fizisko personas datu apstrādes likumu (turpmāk — Datu likums) un starptautiskā standarta LVS EN ISO/IEC 17065:2013 prasībām (Atbilstības novērtēšana — Prasības institūcijām, kas sertificē produktus, procesus un pakalpojumus (turpmāk — ISO/IEC 17065)), nosaka un apstiprina Datu regulas 43. panta 3. punktā minētos sertifikācijas struktūru akreditācijas kritērijus.

Ņemot vērā, ka Datu regulā ir noteiktas papildu akreditācijas prasības, kas jāievēro, piemērojot ISO/IEC 17065, šajā dokumentā Inspekcija izklāsta prasības personas datu aizsardzībai un uzsver papildu prasības, tām, kas jau ir noteiktas ISO/IEC 17065. Prasībās ievērota ISO/IEC 17065 struktūra, nodaļās, kurās papildus prasības ISO 17065 izvirzītajām prasībām nav, norādot, ka nodaļā nav papildus prasības.

Sertifikācijas mehānisms, ar kuru sertifikācijas struktūras, kas akreditētas saskaņā ar ISO/IEC 17065, izdos un atjaunos sertifikātus, ir papildu instruments, lai pierādītu, ka personas datu apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst Datu regulai, tādējādi novērtējot pārziņu centienus nodrošināt datu aizsardzības procesu atbilstību.

Izstrādājot šo dokumentu, Inspekcija ņem vērā Eiropas Datu aizsardzības kolēģijas² (turpmāk — EDAK) izstrādātās Pamatnostādnes 4/2018 par sertifikācijas struktūru akreditāciju saskaņā ar Datu regulas 43. pantu.

Ievērojot Datu regulas 43. panta 1., 2. un 3. punktu, tostarp to, ka sertifikācijas struktūras akreditāciju veic, pamatojoties uz Inspekcijas apstiprinātiem kritērijiem, ja uzņēmums vēlas saņemt akreditāciju, lai darbotos kā sertifikācijas struktūra, papildus ISO /IEC 17065 prasībām ir jāatbilst šajā dokumentā noteiktajām prasībām. Plašāka informācija pieejama Inspekcijas un valsts aģentūras “Latvijas Nacionālais akreditācijas birojs” (turpmāk — LATAK) mājaslapā.

Inspekcija kā datu aizsardzības uzraudzības iestāde un LATAK kā valsts akreditācijas struktūra ir noslēguši starpresoru vienošanos, kurā izklāstīti sadarbības un koordinācijas noteikumi starp abām pusēm akreditācijas procedūru ietvaros.

Inspekcijai ir tiesības izdot papildu kritērijus, kas ievērojami akreditācijas procesā, un nepieciešamības gadījumā šie kritēriji var tikt pārskatīti.

¹Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (95/46. gada aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)

² Pamatnostādnes 4/2018 par sertifikācijas struktūru akreditāciju saskaņā ar Vispārīgās datu aizsardzības regulas (2016/679) 43. pantu

SAĪSINĀJUMI

Sertifikācijas institūcija (struktūra) — trešās personas atbilstības novērtēšanas struktūra, kas izmanto sertifikācijas mehānismus un kas atbilst sertifikācijas sistēmas prasībām;

Nacionālā akreditācijas iestāde — valsts aģentūra “Latvijas Nacionālais akreditācijas birojs” (LATAK);

Datu valsts inspekcija — Inspekcija;

Akreditācija — valsts akreditācijas struktūra (LATAK) veikta atestācija par sertifikācijas institūcijas kompetenci un spēju veikt specifiskas atbilstības novērtēšanas; darbības.

Sertifikācija — novērtējums un objektīvs, trešās personas apliecinājums, ka ir pierādīta sertifikācijas kritēriju izpilde;

Kritēriji vai sertifikācijas kritēriji — kritēriji, pēc kuriem tiek veikta sertifikācija (atbilstības novērtēšana). **Sertifikāts** — LATAK akreditētas sertifikācijas struktūras izsniegts sertifikāts par datu aizsardzības prasību atbilstību Datu regulas prasībām, kas tiek izsniegts uz 3 gadiem, ar iespēju to pagarināt. Sertifikāta iegūšana ir brīvprātīga;

Sertifikācijas priekšmets — tādas apstrādes darbības, kas pārzinim vai apstrādātājam apliecina produktu, procesu vai pakalpojumu, vai produktu, procesu vai pakalpojumu, ar kuru palīdzību ir iespējams nodrošināt atbilstību Datu regulai;

Sertifikācijas līgums — līgums, kas noslēgts starp sertifikācijas iestādi un klientu par sertifikācijas darbību veikšanu klientam;

Sertifikācijas sistēma — sertifikācijas sistēma, kas saistīta ar konkrētiem produktiem, procesiem un pakalpojumiem, uz kuriem attiecas tās pašas noteiktās prasības, noteikumi un procedūras;

Sertifikācijas procedūra — dokuments, kas atspoguļo sertifikācijas procesu;

Akreditācijas procedūra — dokuments, kurā ir formulēts akreditācijas process, kā arī tā mērķis, izpildes laiks, akreditācijas procesā plānotās LATAK darbības klienta novērtēšanai;

Klients — organizācija vai persona, ko sertifikācijas struktūra novērtē attiecībā uz sertifikācijas kritēriju un/vai produktu piemērojamību, lai nodrošinātu Datu regulas prasības. Definīcija “klients” tiek izmantota, lai identificētu gan sertifikācijas struktūras pieteikuma iesniedzēju, gan sertificēto struktūru.

Pieteikums — sertifikācijas struktūras pieteikums uz sertifikācijas pakalpojumu sniegšanas akreditāciju vai tās akreditācijas atjaunošanu.

1. DARBĪBAS JOMA

Papildus ISO/IEC 17065 jānorāda, ka saskaņā ar Datu regulas 42. panta 1. punktu sertifikācija attiecas tikai uz apstrādes darbībām, ko veic pārziņi un apstrādātāji. Ņemot vērā to, ka sertifikācija ietilpst Datu regulas darbības jomā, produktu, procesu un pakalpojumu sertifikācijas procesā visaugstāko prioritāti piešķir atbilstībai Datu regulas prasībām.

2. NORMATĪVĀ ATSAUCE

Datu regula prevalē pār ISO/IEC 17065. Ja papildu prasības vai sertifikācijas mehānisms attiecas uz citiem ISO standartiem, tos interpretē saskaņā ar Datu regulā noteiktajām prasībām.

3. TERMINI UN DEFINĪCIJAS

Piemēro ISO/IEC 17065 izmantotos terminus un definīcijas, ja vien tie neatšķiras no Datu regulas noteikumiem un definīcijām, kā tas interpretēts EDAK pamatnostādnēs par akreditāciju un sertifikāciju³.

4. VISPĀRĪGĀS AKREDITĀCIJAS PRASĪBAS

4.1 Juridiskie un līgumiskie jautājumi

4.1.1 Juridiskā atbildība

4.1.1.1. Sertifikācijas struktūra spēj demonstrēt labu reputāciju personas datu aizsardzības jomā, apliecinot, ka uz to neattiecas Inspekcijas uzsāktās pārbaudes un/vai izmeklēšanas, un sertifikācijas struktūra pēdējo četru gadu laikā nav administratīvi sodīta par personas datu aizsardzības pārkāpumiem.

4.1.1.2. Sertifikācijas struktūra ievēro papildu prasības attiecībā uz Datu regulas un attiecīgā gadījumā citu tiesību aktu piemērošanu, kas reglamentē personas datu aizsardzību, un ka sertifikācijas saņemšanai pieteiktās procedūras un dokumenti tiek laikus atjaunināti, par minētās prasības ievērošanu iesniedz apliecinājumu Inspekcijai;

4.1.1.3. Sertifikācijas struktūra iesniedz apliecinājumu, ka, apstrādājot personas datus, tā ievēro Datu regulu un attiecīgā gadījumā citus tiesību aktus, kas reglamentē personas datu aizsardzību.

4.1.2 Sertifikācijas līgums

Papildus ISO/IEC 17065 prasībām sertifikācijas struktūra, iesniedzot Inspekcijai līguma/u projektu/us, pierāda, ka tās sertifikācijas līgumi:

4.1.2.1. satur prasību, ka Klients vienmēr ievēro gan vispārīgās sertifikācijas prasības standarta ISO 17065 4.1.2.2. punkta a) apakšpunkta izpratnē, gan sertifikācijas struktūras noteiktos un Inspekcijas apstiprinātos sertifikācijas kritērijus;

4.1.2.2. paredz Klienta pienākumu nodrošināt Inspekcijai pilnīgu pārredzamību attiecībā uz sertifikācijas procedūru, tai skaitā piekļuvi nepieciešamajai informācijai, tai skaitā līgumā noteiktajiem konfidencialajiem jautājumiem, lai pārbaudītu Klienta atbilstību datu aizsardzības prasībām⁴;

4.1.2.3. nesatur prasības, kas samazina Klienta vai sertifikācijas institūcijas atbildību, kas izriet no Datu regulas, un neietekmē Inspekcijas pilnvaras un/vai uzdevumus saskaņā ar Datu regulas 42. panta 5. punktu un 55.–58. pantu;

4.1.2.4. nosaka, ka Klients sniedz sertifikācijas institūcijai visu informāciju un piekļuvi savām apstrādes darbībām, kas nepieciešamas sertifikācijas procedūras veikšanai⁵;

4.1.2.5. nosaka, ka Klientam ir jāievēro noteiktie termiņi un procedūras, kas izriet no sertifikācijas kritērijiem vai citiem noteikumiem;

³ Pamatnostādnes 4/2018 par sertifikācijas struktūru akreditāciju saskaņā ar Vispārīgās datu aizsardzības regulas (2016/679) 43. pantu

⁴ Nodrošināt Datu regulas 42. panta 7. punkta un 58. panta 1. punkta c) apakšpunkta piemērošanu.

⁵ Saskaņā ar Datu regulas 42. panta 6. punktu

4.1.2.6. satur noteikumus par derīgumu, atjaunošanu (tostarp atjaunotā sertifikāta derīguma termiņa noteikšanu) un atsaukšanu, kā arī noteikumus, kas nosaka atkārtotas novērtēšanas vai pārskatīšanas intervālus, tostarp, kādas sekas rodas sertifikācijas apturēšanas, atsaukšanas vai anulēšanas gadījumā un kādi termiņi ir saistoši Klientam šādos gadījumos⁶;

4.1.2.7. paredz, ka Klients dod sertifikācijas institūcijai tiesības atklāt EDAK visu informāciju par sertifikāciju, t. i., sertificējamās struktūras nosaukumu, struktūru, kas izdevusi sertifikātu, sertifikāta datumu, sertificētās personas datu apstrādes darbības aprakstu un attiecīgā gadījumā sertifikāta atsaukšanas datumu un šādas atsaukšanas iemeslus vai sertifikāta apturēšanas datumu, termiņu vai iemeslus saskaņā ar Datu regulas 42. panta 8. punktu. Sertificējamā institūcija līgumā apliecina, ka tā saprot, ka informācija tiks iekļauta reģistrā, kas ir publiski pieejams EDAK tīmekļa vietnē;

4.1.2.8. nosaka, ka Klienta pienākums ir apliecināt gatavību sertifikāta derīguma laikā veiktai atbilstības procesu uzraudzībai, atbilstības novērtēšanas darbībām un īstenoto procesu pārbaudēm;

4.1.2.9. ietver sertifikācijas institūcijas sūdzību pārvaldības struktūru un procedūras, kā arī nepieciešamos piesardzības pasākumus sūdzību izskatīšanai, tostarp pienākumu dokumentēt visas iesniegtās sūdzības sertifikācijas jomā un nodrošināt pasākumus saņemto sūdzību izskatīšanai, kā arī nodrošināt pārredzamu un viegli pieejamu sūdzību izskatīšanas procesu⁷;

4.1.2.10. paredz, kādas sekas ir sertifikācijas struktūras akreditācijas atsaukšanas vai apturēšanas gadījumā, tostarp ietekme uz Klientu, tā sertifikāciju un iespējamiem turpmākiem pasākumiem, kas varētu tikt veikti;

4.1.2.11. nosaka, ka Klients apņemas paziņot sertifikācijas institūcijai par visiem uzraudzības iestāžu vai tiesas konstatētajiem Datu regulas un citu personas datu aizsardzību regulējošo tiesību aktu pārkāpumiem, kas var ietekmēt atbilstības novērtēšanu. Iepriekš minētā informācija tiek sniegta nekavējoties pēc tam, kad Klientam kļūst pieejama informācija par konstatēto pārkāpumu;

4.1.2.12. nosaka, ka Klients apņemas paziņot sertifikācijas institūcijai par būtiskām izmaiņām tā faktiskajā vai juridiskajā situācijā un produktos, procesos un pakalpojumos, kas ir nozīmīgi sertifikācijas procesam vai atbilstībai sertifikācijas kritērijiem, un kā tiek nodrošināta nepieciešamo izmaiņu ieviešana.

4.1.2.13. Paredz 7.4. punktā noteiktās saistošās novērtēšanas metodes sertifikācijas priekšmeta atbilstības novērtēšanai.

4.1.3. Datu aizsardzības zīmogu un zīmju izmantošana.

Sertifikācijas institūcija iesniedz apliecinājumu, ka sertifikātus, zīmogus un marķējumus izmanto tikai saskaņā ar Datu regulas 42. un 43. pantu un EDAK Pamatnostādnēm Nr. 4/2018 par sertifikācijas struktūru akreditāciju saskaņā ar Datu regulas 43. pantu.

4.2. Objektivitātes pārvaldība

4.2.1. Sertifikācijas struktūra iesniedz Inspekcijai informāciju (dibināšanas dokumentus, procedūras), kas apstiprina sertifikācijas struktūras neatkarību, tostarp finansējuma avotus, un nodrošina interešu konfliktu neesamību.

4.2.2. Sertifikācijas struktūra sniedz paziņojumu, ka tā ir trešā persona attiecībā uz Klientu ISO 17000:2020 nozīmē.⁸

⁶Saskaņā ar Datu regulas 42. panta 7. punktu un 43. panta 4. punktu

⁷Saskaņā ar Datu regulas 43. panta 2. punkta d) apakšpunktu

⁸Trešā puse ir iestāde, kas ir neatkarīga trešā persona, kas pārbauda sertifikācijas apstākļus un ir neatkarīga no pārbaudes priekšmeta piemērotāja interesēm. Atbilstoši Eiropas Parlamenta un Padomes 2008.gada 9.jūlija lēmuma Nr. 768/2008/EK par produktu tirdzniecības sistēmu un ar ko atceļ Padomes lēmumu 93/465/EEK, I. pielikuma R17 panta 3.punktam atbilstības novērtēšanas struktūrai ir jābūt trešajai personai, kas ir neatkarīga no organizācijas vai produkta, kam tā veic novērtēšanu. Regulas 17 panta 4.punkts nosaka, ka Atbilstības novērtēšanas struktūra, tās augstākā vadība un darbinieki, kas ir atbildīgi par atbilstības novērtēšanas uzdevumiem, nav vērtējamo produktu konstruktori, ražotāji, piegādātāji, uzstādītāji, pircēji, īpašnieki, lietotāji vai apkalpotāji, ne arī to pilnvaroti pārstāvji. Tas neliedz izmantot novērtētos produktus, kas ir vajadzīgi atbilstības novērtēšanas struktūras darbībai, vai izmantot šādus produktus personiskiem mērķiem.

4.2.3. Sertifikācijas struktūra nodrošina interešu konfliktu novēršanas procedūru iekļaušanu iekšējos procesos un, ja nepieciešams, iesaistīto subjektu institucionālajā dalījumā.

4.2.4. Sertifikācijas struktūra nodrošina interešu konflikta novēršanas procesa dokumentāciju.

4.2.5. Sertifikācijas struktūras iekšējās kontroles mehānismi garantē, ka sertifikācijas struktūra nav darījumu attiecībās ar Klientu.

4.2.6. Sertifikācijas struktūra nodrošina, ka tiek novērsti interešu konflikti⁹, nodalot procesus un pienākumus, un pierāda, iesniedzot attiecīgus dokumentus, ka sertifikācijas struktūras un saistītās juridiskās personas darbinieki ir nošķirti un nepiedalās sertifikācijas, vērtēšanas un verificācijas procesā.

4.2.7. Sertifikācijas struktūras augstākajai vadībai ir pienākums ievērot līgumā vai sertifikācijas struktūras statūtos noteikto neitralitāti darbībās un lēmumu pieņemšanā.

4.2.8. Sertifikācijas struktūra iesniedz Inspekcijai procedūras interešu konfliktu novēršanai un konstatēto interešu konfliktu pārvaldībai.

4.3. *Saistības un finansējums*

4.3.1. Sertifikācijas struktūra iesniedz apliecinājumu un ir gatava demonstrēt, ka tai ir finanšu resursi, kas atbilst tās darbības jomai un apjomam, lai segtu savas saistības.

4.3.2. Sertifikācijas struktūra Inspekcijai iesniedz derīgu civiltiesiskās atbildības apdrošināšanas līgumu.

4.4. *Nediskriminējoši nosacījumi*

Nav papildu prasību attiecībā uz ISO/IEC 17065

4.5. *Konfidencialitāte*

Nav papildu prasību attiecībā uz ISO/IEC 17065

4.6. *Viegli publiski pieejama informācija*

4.6.1. Sertifikācijas struktūra iesniedz procedūru, atbilstoši kurai tā dara viegli pieejamu informāciju sabiedrībai, publicējot savā tīmekļa vietnē:

4.6.1.1. izmantotos sertifikācijas kritērijus;

4.6.1.2. visas (spēkā esošās un iepriekšējās) apstiprināto kritēriju versijas, kas izmantotas Datu regulas 42. panta 5. punkta nozīmē;

4.6.1.3. visas sertifikācijas procedūras, kas tiek izmantotas, lai pārbaudītu Klienta atbilstību sertifikācijas kritērijiem;

4.6.1.4. informāciju par sūdzību izskatīšanas procedūrām un pārsūdzībām saskaņā ar Datu regulas 43. panta 2. punkta d) apakšpunktu;

4.6.1.5. sertificēto klientu reģistrs;

4.6.1.6. novērtējuma ziņojuma kopsavilkumu par to, kas ir apliecināts un kā tas novērtēts. Novērtējuma ziņojuma kopsavilkumā iekļauj šādu informāciju, kas attiecas uz novērtējumu:

4.6.1.6.1. sertifikācijas apjomu un sertifikācijas priekšmeta aprakstu;

⁹ Sertifikācijas institūcija (struktūra), kas pieder juridiskai personai (piemēram, biedrībai vai korporācijai saskaņā ar publiskajām tiesībām) vai to kontrolē juridiska persona, vai ir kādas citas attiecības ar juridisku personu, kuras dalībnieki vai akcionāri ir ražotāji, piegādātāji, pārstrādātāji, vai pārziņi, kurus ir sertificējusi šī sertifikācijas struktūra, var tikt uzskatīta par neatkarīgu trešo personu tikai tad, ja tās neatkarība ir nodrošināta, ievērojot Regulas 43.panta 2.punkta "a" apakšpunktā noteikto un vai tās interešu konfliktu neesamība ir demonstrēta, ievērojot DIN EN ISO/IEC 17065 3.13.punktu.

4.6.1.6.2. attiecīgos sertifikācijas kritērijus (tostarp to versiju vai funkcionālo statusu);

4.6.1.6.3. veiktās novērtēšanas metodes un testi;

4.6.1.6.4. novērtēšanas rezultāti.

4.6.2. Sertifikācijas struktūra iesniedz Inspekcijā procedūras, lai nodrošinātu informācijas pieejamību pēc pieprasījuma attiecībā uz šādu informāciju:

4.6.2.1. sertifikācijas shēmu;

4.6.2.2. Klienta atbilstības sertifikācijas kritērijiem novērtēšanas standartu;

4.6.2.3. minimālās prasības sertifikācijas līgumiem;

4.6.2.4. konkrētu sertifikātu un saistīto publikāciju pēcpārbaudi vai attiecīgā gadījumā īpašas sūdzības par sertifikātu.

4.6.3. Sertifikācijas struktūras tīmekļa vietnei jābūt pieejamai formā, kas ir līdzvērtīga tai, kuru izmanto, lai reklamētu vai uzskaitītu sertifikācijas struktūras pakalpojumus. Sertifikācijas institūcija Inspekciju informē par tīmekļvietnes pieejamību, iesniedzot saiti uz to.

5. STRUKTURĀLĀS PRASĪBAS

5.1. Organizatoriskā struktūra un augstākā vadība

Nav papildu prasību attiecībā uz ISO/IEC 17065

5.2. Objektivitātes nodrošināšanas mehānismi

Nav papildu prasību attiecībā uz ISO/IEC 17065

6. PRASĪBAS ATTIECĪBĀ UZ RESURSIEM

6.1. Sertifikācijas struktūras personāls

6.1.1. Sertifikācijas struktūra nodrošina un spēj pierādīt, ka sertifikācijas struktūras personāla kvalifikācija un profesionālā pieredze atbilst šādām minimālajām prasībām:

6.1.1.2. ir atbilstošas, pastāvīgas un piemērotas zināšanas par sertifikācijas objektu, ņemot vērā Datu regulas 43. panta 2. punkta a) apakšpunktu, vai ir 2 gadu pieredze darbībā, kas saistītas ar sertificējamo objektu;

6.1.1.3. ir neatkarīgi un to funkcijas un atbildība sertifikācijas struktūras darbībā neradītu interešu konfliktu, ņemot vērā Datu regulas 43. panta 2. punkta a) apakšpunktu un 43. panta 2. punkta e) apakšpunktu;

6.1.1.4. ir apņēmušies ievērot Datu regulas 42. panta 5. punktā noteiktās prasības saskaņā ar Datu regulas 43. panta 2. punkta b) apakšpunktu;

6.1.1.5. ir atbilstošas, pastāvīgas un piemērotas zināšanas par personas datu tehniskajiem un organizatoriskajiem drošības pasākumiem, tiem izvirzītajām prasībām, un, ja nepieciešams, piemērošanas pieredze.

6.1.2. Sertifikācijas struktūrai jāspēj pierādīt, ka tās personāls ar tehnisko pieredzi:

6.1.2.1. ir ieguvis kvalifikāciju attiecīgajā tehnisko zināšanu jomā vismaz līdz Eiropas kvalifikāciju ietvarstruktūras (*European Qualifications Framework*) sestajam līmenim vai atzītajam aizsargātajam nosaukumam (piemēram, dipl. Ing.) attiecīgajā reglamentētajā profesijā vai vismaz 5 gadu profesionālo pieredzi informācijas tehnoloģiju jomā.

6.1.2.2. darbiniekiem, kas atbild par sertifikācijas lēmumiem, jābūt ievērojamai profesionālai pieredzei datu aizsardzības pasākumu noteikšanā un īstenošanā;

6.1.2.3. darbiniekiem, kas ir atbildīgi par izvērtēšanu, jābūt vismaz 2 gadu profesionālai pieredzei tehnisko datu aizsardzībā un pieredzei sertifikācijas, audita vai salīdzināmās procedūrās un pieredzei darbā ar to;

6.1.2.4. ir jāpierāda, ka viņi uzlabo savu kvalifikāciju attiecīgajā jomā, kas saistīta ar tehniskajām un audita zināšanām, pastāvīgi piedalās profesionālās pilnveides programmās.

6.1.3. Sertifikācijas struktūrai jāspēj pierādīt, ka tās darbinieki ar juridiskajām zināšanām:

6.1.3.1. ir pabeiguši juridiskās studijas Eiropas Savienības vai Latvijas Republikas atzītā universitātē (vismaz astoņus semestrus) un pēc studiju pabeigšanas ir piešķirts akadēmiskais maģistra (LL.M.) vai līdzvērtīgs grāds vai iegūta vismaz 5 gadu profesionālā pieredze;

6.1.3.2. par sertifikācijas lēmumiem atbildīgajiem darbiniekiem ir vismaz 3 gadu pieredze datu aizsardzības tiesību jomā;

6.1.3.3. darbiniekiem, kuri ir atbildīgi par izvērtēšanu, ir vismaz 2 gadu profesionālā pieredze datu aizsardzības tiesību jomā un zināšanas un pieredze saistībā ar salīdzināmām procedūrām (piemēram, sertifikāciju un/vai revīziju) un/vai sertificētu objektu;

6.1.3.4. personāls turpina uzturēt savu kompetenci attiecīgajā jomā attiecībā uz juridiskajām zināšanām un zināšanām par audita veikšanu, pastāvīgi piedalās profesionālās pilnveides programmās.

6.1.4. Ārvalstīs iegūto izglītības dokumentu akadēmiskā atzīšana notiek Izglītības likumā un Augstskolu likumā noteiktajā kārtībā, sazinoties ar Akadēmiskās informācijas centru. Ja izglītības dokuments ir pielīdzināts, Klients iesniedz Inspekcijai attiecīgās iestādes lēmumu par izglītības dokumenta atzīšanu.

6.1.5. Sertifikācijas institūcija nepieciešamības gadījumā var paļauties uz citu personu tehniskajām un profesionālajām prasmēm. Ja tiek piesaistīti apakšuzņēmēji, Inspekcijai iesniedz apakšuzņēmēju apliecinājumu par gatavību veikt tiem nodotos darbus vai nodot resursus sertifikācijas institūcijai.

6.1.8. Sertifikācijas institūcija izstrādā un Inspekcijai iesniedz kārtību, kas paredz regulāras personāla apmācības un kvalifikācijas uzlabošanu, nodrošinot personāla zināšanu saglabāšanu un pilnveidošanu.

6.2. Resursi izvērtēšanai

Nav papildu prasību attiecībā uz ISO/IEC 17065

7. PRASĪBAS ATTIECĪBĀ UZ PROCESU

7.1. Vispārīgi noteikumi

7.1.1 Sertifikācijas struktūra, veicot Datu regulas 43. panta 2. punkta c) un d) apakšpunktā minētās procedūras, ievēro Inspekcijas noteiktās papildu prasības, kā paredzēts Datu regulā (43. panta 1. punkta b) apakšpunkts), jo īpaši, lai sertifikācijas struktūras uzdevumi un pienākumi neradītu interešu konfliktu (saskaņā ar Datu regulas 43. panta 2. punkta e) apakšpunktu), un iesniedz Inspekcijai sertifikācijas institūcijas izstrādātas procedūras, kuras demonstrē, ka:

7.1.2. Sertifikācijas struktūra sertifikācijas procesā:

7.1.2.1. ir saņēmusi Inspekcijas atzinumu par sertifikācijas kritēriju atbilstību;

7.1.2.2. ievēro tās izstrādātos un Inspekcijas apstiprinātos sertifikācijas kritērijus, lai novērtētu Klienta atbilstību Datu regulai;

7.1.2.3. ņem vērā EDAK pamatnostādnes;

7.1.2.3. pieprasa jaunu Inspekcijas atzinumu par atbilstību kritērijiem ikreiz, kad sertifikācijas kritēriji tiek būtiski mainīti.

7.1.3. Ja sertifikācijas struktūra plāno darboties citās dalībvalstīs, tā iesniedz apliecinājumu, ka ir saņēmusi nepieciešamo apstiprinājumu no attiecīgajām uzraudzības iestādēm vai iesniedz pieteikumu Eiropas datu aizsardzības zīmoga saņemšanai saskaņā ar Datu regulas 42. panta 5. punktu. Ja sertifikācijas struktūra plāno darboties citās dalībvalstīs, par to iepriekš jāinformē visas attiecīgās uzraudzības iestādes.

7.1.4. Sertifikācijas struktūra iesniedz procedūru, kas demonstrē, ka tā apņemas organizēt izmeklēšanu pret klientu par personas datu aizsardzības tiesiskā regulējuma pārkāpumiem sertifikācijas un novērtēšanas ietvaros, ja klients paziņo, ka uz viņu tiek veikta Inspekcijas izmeklēšana, vai Inspekcija informē sertifikācijas struktūru par izmeklēšanu.

7.1.5. Sertifikācijas struktūra iesniedz procedūru, kas demonstrē, kā tā nodrošinās sadarbību ar Inspekciju, veicot izmeklēšanu par klientiem, kurus tā ir sertificējusi un iesniegs Inspekcijai novērtējuma ziņojumu par veikto izmeklēšanu, kurā secināts, vai klients joprojām atbilst sertifikācijas nosacījumiem.

7.1.6. Sertifikācijas struktūra izstrādā un iesniedz procedūru, kas paredz efektīvus saziņas mehānismus starp sertifikācijas iestādi un klientu, kas paātrina apstrādi un reaģēšanu uz informācijas pieprasījumiem par pašreizējo procedūru vai citu būtisku informāciju.

7.2. Sertifikācijas pieteikums

7.2.1. Sertifikācijas struktūra pieprasa, lai Klienti sertifikācijas pieteikumā identificētu:

7.2.1.1. sertifikācijas apjomu, tai skaitā detalizētu sertifikācijas priekšmeta aprakstu, tai skaitā saskarnes, saziņas ar citām sistēmām un organizācijām, protokolus un citus saistošos noteikumus par sertifikācijas priekšmetu;

7.2.1.2. kopīgos pārziņus un/vai datu apstrādātājus. Ja apstrādātājs ir Klients, ir jāapraksta tā pienākumi un uzdevumi. Iekļauj pārziņa/apstrādātāja līgumu, tostarp kopīgo pārziņu kopiju un to īpašo kārtību.

7.2.1.3. Lai apliecinātu 7.2.1. prasības izpildi, sertifikācijas institūcija Inspekcijai iesniedz apliecinājumu, ka sertifikācijas pieteikumiem tiks izvirzītas minētās prasības vai iesniedz pieteikuma veidlapas paraugu, ja tāda tiks izmantota.

7.3. Pieteikuma pārskatīšana

Papildus ISO/IEC 17065 7.3. punkta e) punkta prasībām sertifikācijas institūcijai, pārskatot Klienta pieteikumu, jāgūst pārliecība, ka Klientam ir sertifikācijas izpildei nepieciešamā gan tehniskā, gan juridiskā kompetence datu aizsardzības jomā. Sertifikācijas institūcija iesniedz procedūras aprakstu, kas apliecina, kā sertifikācijas institūcija nodrošinās prasības izpildi.

7.4. Novērtējums

7.4.1. Sertifikācijas struktūra iesniedz Inspekcijā sertifikācijas shēmu, kurā parādīts, kā tajā ir integrētas šādas Klienta novērtēšanas mehānismos iekļautās metodes:

7.4.1.1. novērtējums par apstrādes darbību nepieciešamību un samērīgumu saistībā ar to nolūku un attiecīgajiem datu subjektiem;

7.4.1.2. riska apkopošanas un analīzes novērtējums un seguma un sastāva novērtēšanas metode, ko veic juridisko, tehnisko un organizatorisko seku novērtēšanai, ja sertifikācijas priekšmetam ir piemērojami Datu regulas 24., 25., 32., 35. un 36. panta normatīvie noteikumi;

7.4.1.3. novērtējums par tiesiskās aizsardzības līdzekļiem, tostarp garantijām, aizsardzības pasākumiem un procedūrām, lai nodrošinātu personas datu aizsardzību saistībā ar apstrādi, ko piemēro sertifikācijas subjektam, un lai pierādītu, ka šādi pasākumi atbilst datu aizsardzības tiesiskajam režīmam;

7.4.1.4. kā tiek nodrošināta salīdzināmu metožu izmantošana novērtēšanas un uzraudzības mehānismos salīdzināmās situācijās. Jebkādas atkāpes no šīs procedūras ir jāpamato sertifikācijas struktūrai;

7.4.1.5. kā drošības aizsardzības, garantijas un procesa īstenošanas pasākumi, kas nodrošina personas datu aizsardzību un atbildības prasības sertifikācijas subjektiem, tiek novērtēti visā apstrādes laikā;

7.4.1.6. jādokumentē izmantotās vērtēšanas metodes un vērtēšanas rezultāti.

7.4.2. Sertifikācijas institūcija iesniedz procesu aprakstu, ar kuru apliecina, ka sertifikācijas institūcijai sertifikācijas procesa novērtēšanas laikā ir tiesības pieprasīt Klientam papildu informāciju un dokumentus. Procesu aprakstā paredzēts, ka Sertifikācijas institūcijai ir tiesības atcelt sertifikācijas novērtēšanas procesu, ja Klients nesniedz tai pieprasīto informāciju un dokumentāciju.

7.4.3. Sertifikācijas struktūra iesniedz procesu aprakstu, kas nosaka regulāru izmantoto metožu pārskatīšanu, ņemot vērā tehnoloģiju attīstību un izmaiņas tiesiskajā regulējumā.

7.4.4. Iesaistot apakšuzņēmējus:

7.4.4.1. Sertifikācijas struktūra informē Inspekciju par visiem apakšuzņēmējiem un uzdevumiem, ko sertifikācijas struktūra ir nodevusi katram apakšuzņēmējam;

7.4.4.2. Sertifikācijas struktūra iesniedz apakšuzņēmēju rakstiskus apstiprinājumus par apakšuzņēmēja gatavību veikt apakšuzņēmējiem nododamo uzdevumu sarakstā norādītos darbus un/vai nodot darbu veikšanai nepieciešamos resursus sertifikācijas struktūras rīcībā.

7.4.4.3. apakšuzņēmējam jāievēro Datu regula, šā dokumenta prasības, ciktāl tās attiecas un apakšuzņēmējam nodoto uzdevumu izpildē, jānodrošina objektivitātes pārvaldība savā struktūrā, un jāspēj demonstrēt laba reputācija datu aizsardzības jomā, ko sertifikācijas institūcija Inspekcijai apliecina, iesniedzot starp apakšuzņēmēju un sertifikācijas institūciju noslēgtu vienošanos, kas paredz minētos nosacījumus.

7.4.4.4. Sertifikācijas struktūra saglabā pilnu atbildību par lēmumu pieņemšanu, iesaistot apakšuzņēmējus.

7.4.5. Sertifikācijas struktūra iesniedz Inspekcijai procedūru, kurā norāda, cik liela nozīme attiecībā uz sertifikāciju ir tās atbilstībai citiem kvalitātes standartiem (piemēram, ISO 27001, ISO 27002) un šīs atbilstības novērtējumam, tostarp to, kādus sertifikātus var ņemt vērā novērtēšanas procesā, kā un kādā mērā tie ietekmē novērtēšanas procesu:

7.4.5.1 Procedūrā var paredzēt citu sertifikātu izmantošanu, ja:

7.4.5.1.1. cita sertifikācija saskaņā ar Datu regulas 42. pantu attiecas uz daļu no sertifikācijas priekšmeta, un to var uzskatīt par daļēji būtisku jaunajam sertifikācijas novērtēšanas procesam;

7.4.5.1.2. ja atbilstības novērtēšanā un jau novērtētās sertifikācijas kontekstā tiek ņemta vērā cita esoša sertifikācija, procedūrā paredz sertifikācijas struktūras pienākumu veikt izlases veida pārbaudes un novērtēt esošo sertifikāciju atbilstoši prasībām (attiecībā uz uzsākto sertifikāciju);

7.4.5.1.3. procedūra nosaka, kā tiks noteikti sertifikācijas derīguma termiņi. Sertifikāta derīguma termiņu nosaka, ņemot vērā esošā sertifikāta īsāko termiņu. Tomēr pieejamie derīgie sertifikāti nevar automātiski nozīmēt, ka sertificētais priekšmets atbilst sertifikācijas kritērijiem un ka Datu regulas sertifikācija ir atkarīga no citu veidu sertifikācijas derīguma;

7.4.5.1.4. procedūra nosaka mehānismu pilnīgas informācijas saņemšanai par citas akreditētas sertifikācijas struktūras esošās sertifikācijas novērtējumu, kas ļauj novērtēt šīs esošās sertifikācijas darbību un rezultātus. Ja pārbaudē atklājas novirzes no prasībām vai citas neatbilstības, procedūrā paredz, ka novērtējumu attiecina arī uz esošo sertifikācijas procedūru un, ja nepieciešams, uz visu sertifikācijas subjektu.

7.4.6. Sertifikācijas struktūra nosaka nosacījumus un procedūras informācijas izmantošanai par jebkuru iepriekš iegūtu sertifikāciju saskaņā ar Datu regulas 42. un 43. pantu, ko klients vēlas nodot vai ņemt vērā.

7.4.7. Sertifikācijas institūcija (struktūra) nodrošina pārskatatbildību attiecībā uz atbilstības novērtēšanas darbībām, un Inspekcija iesniedz procesa aprakstu, kurā paredzēts, ka, novērtējot atbilstību, tiks fiksēts:

7.4.7.1. uz kāda pamata tika sagatavots novērtējuma plāns, ja nepieciešams, ar atbilstošām atsaucēm, likumiem un specifiskiem tehniskiem standartiem;

7.4.7.2. izvēlēto metožu izmantošana pārbaudēs un atbilstības novērtēšanas procesos;

7.4.7.3. testu un standartu uzlabojumu dokumentācija, norādot attiecīgā pielāgojuma laiku un iemeslus;

7.4.7.4. kārtību atbilstības novērtēšanas pārraudzībai, ko veic trešā persona.

7.4.8. Sertifikācijas struktūra iesniedz procedūru novērtējuma ziņojuma, kurā dokumentē novērtēšanas procesu, sagatavošanai.

7.4.9. Sertifikācijas struktūra iesniedz Inspekcijai procedūru, ar kuru demonstrē, ka pēc pieprasījuma Inspekcijai ir pilnībā pieejama novērtējuma (sertifikācijas procesa) dokumentācija.

7.5. Sertifikātu pārskatīšana

Sertifikācijas institūcija iesniedz procedūras attiecīgo sertifikātu izsniegšanai, regulārai pārskatīšanai un atsaukšanai saskaņā ar Datu regulas 43. panta 2. punktu un 43. panta 3. punktu.

7.6. Sertifikācijas lēmums

7.6.1. Sertifikācijas struktūra iesniedz procesu aprakstu un citus apliecinājošus dokumentus, kas atspoguļo, kā tiek nodrošināta tās neatkarība un atbildība par individuālo sertifikācijas lēmumu.

7.6.2. Lai nodrošinātu sertifikācijas procesa pārredzamību, sertifikācijas institūcija nosaka un iesniedz Inspekcijai kārtību, kādā pirms lēmuma par Klienta sertifikāciju, sertifikāta atjaunošanu vai sertifikāta paplašināšanu pieņemšanas tiek informēta Inspekcija.

7.6.3. Pirms lēmuma pieņemšanas sertifikācijas struktūrai ir jāpārlicinās, ka Inspekcija nav uzsākusi izmeklēšanu pret klientu par sertifikācijas darbības jomu. Prasību apliecina, iekļaujot tās izpildes kārtību 7.6.2. punktā norādītajā kārtības aprakstā.

7.7. Sertifikācijas dokumenti

7.7.1. Tiek nodrošināts, ka sertifikātā ir norādīts:

7.7.1.1. Sertifikāta derīguma termiņš, kas nepārsniedz trīs gadus;

7.7.1.2. Sertifikācijas priekšmets (attiecīgā gadījumā norādot versijas statusu vai līdzīgus raksturlielumus);

7.7.1.3. Tās organizācijas nosaukums, kas saņem sertifikātu;

7.7.2. Nodrošina, ka lēmumā par sertifikāta piešķiršanu ir norādīts:

7.7.2.1. sertifikācijas uzraudzīšanas pārraudzības periods;

7.7.2.2. Sertifikāta derīguma termiņš, kas nepārsniedz trīs gadus;

7.7.2.3. Sertifikācijas priekšmets (attiecīgā gadījumā norādot versijas statusu vai līdzīgus raksturlielumus);

7.7.2.4. Tās organizācijas nosaukums, kas saņem sertifikātu.

7.8 Informācijas publicēšana

7.8.1. Sertifikācijas struktūra nodrošina novērtējuma ziņojuma kopsavilkuma, kas atbilst 4.6.1.6. punktā noteiktajām prasībām, sagatavošanu un tā publisku pieejamību, publicējot to sertifikācijas struktūras tīmekļa vietnē. Prasības izpildi nodrošina, iesniedzot Inspekcijai 4.6.1. punktā noteikto procedūras aprakstu.

7.8.2. Papildus ISO/IEC 17065/2012 7.8. punktam sertifikācijas struktūra apņemas pa e-pastu informēt visas attiecīgās uzraudzības iestādes par sertifikācijas piešķiršanas vai atsaukšanas iemesliem.

7.9. Uzraudzība

7.9.1. Sertifikācijas struktūra, ievērojot samērīgumu un nediskriminējot, izveido regulārus mehānismus uzraudzībai sertifikācijas derīguma termiņā. Uzraudzības procesu aprakstus iesniedz Inspekcijai.

7.9.2. Uzraudzības pasākumus veic katru gadu, izmantojot uz risku balstītu pieeju, lai noteiktu, vai konkrētos gadījumos uzraudzības darbības jāveic vairāk nekā vienu reizi gadā. Pirmā uzraudzības darbība tiek veikta ne vēlāk kā 12 mēnešus pēc novērtējuma, kas veikts sertifikāta izdošanas nolūkā.

7.9.3. Pēc klienta sertificēšanas uzraudzības periodā jānodrošina, ka tiek veikta Klienta neatbilstību novēršana. Šim nolūkam sertifikācijas struktūra sertifikācijas mehānismā ievieš Klienta informēšanas sistēmu par neatbilstības veidu un termiņiem to novēršanai.

7.9.4. Sertifikācijas institūcija izstrādā kārtību, kādā tā nopietnākas neatbilstības gadījumos papildus profilaksei pieprasa, lai klients veic neatbilstības cēloņu analīzi.

7.10. Izmaiņas, kas ietekmē sertifikāciju

7.10.2. Sertifikācijas struktūra nosaka un iesniedz Inspekcijai procedūras, kas ietver pārejas periodus, apstiprinājuma pieteikuma iesniegšanu Inspekcijā, sertifikāta priekšmeta atkārtotu novērtēšanu un iespējamās atsaukšanas pasākumus, ja tiek konstatētas izmaiņas, kas ietekmē sertifikāciju.

7.10.2. Izmaiņas, kas ietekmē sertifikāciju un kas jāņem vērā sertifikācijas struktūrai:

7.10.2.1. jebkurš personas datu aizsardzības pārkāpuma paziņojums par Datu regulas prasību vai šo kritēriju neievērošanu, kas attiecas uz sertifikācijas apjomu, un kura izvērtēšana ir Inspekcijas vai tiesas kompetence.

7.10.2.2. datu aizsardzībai piemērojamo normatīvo aktu grozījumi;

7.10.2.3. deleģētie vai īstenošanas akti, ko Eiropas Komisija pieņēmusi saskaņā ar Datu regulas 43. panta 8. punktu un 43. panta 9. punktu;

7.10.2.4. EDAK pieņemtie dokumenti;

7.10.2.5. tiesu nolēmumi, kas saistīti ar datu aizsardzību;

7.11. Sertifikācijas izbeigšana, samazināšana, apturēšana vai atsaukšana

7.11.1. Sertifikācijas izbeigšanās, samazināšanas, apturēšanas vai atsaukšanas gadījumā sertifikācijas struktūra nekavējoties rakstiski informē klientu, LATAK un Inspekciju par:

7.11.1.1. sertifikācijas struktūras veiktajiem (vai veicamajiem) pasākumiem (piemēram, atbilstības pārvērtēšana, atbilstības novērtēšanas pārbaude, pieņemtā lēmuma pārskatīšana u. c.) un tā piemērošanas iemeslus, un

7.11.1.2. sertifikāta atjaunošanu, ierobežošanu, apturēšanu vai atsaukšanu.

7.11.2. Sertifikācijas struktūra piemēro samērīgas un pakāpeniskas sankcijas, ja Klients ir noklusējis, slēpis vai kavējis tādas informācijas paziņošanu, kas saistīta ar aktuālām izmeklēšanām saistībā ar sertifikācijas tvērumu, novērtēšanas mērķi un citu informāciju par datu aizsardzības režīma neievērošanu.

7.11.3. Sertifikācijas institūcija izstrādā un iesniedz Inspekcijai kārtību rīcībai, ja Inspekcija devusi rīkojumu atsaukt vai neizsniegt sertifikātu.

7.12. Dokumentu uzskaitē

Sertifikācijas struktūrai ir jānodrošina, ka visa dokumentācija ir pilnīga, saprotama, atjaunināta un gatava revīzijai.

7.13. Sūdzības un apelācijas

7.13.1. Sertifikācijas struktūra nosaka un Inspekcijai iesniedz kārtību, kurā papildus ISO/IEC 17065 attiecībā uz sūdzību izskatīšanu demonstrē:

7.13.1.1. kuras personas ir tiesīgas iesniegt sūdzības un iebildumus par sertifikācijas procesu;

7.13.1.2. kas veic saņemto sūdzību izskatīšanu no sertifikācijas institūcijas puses;

7.13.1.3. kā tiek nodrošināta sertifikācijas darbību nošķiršana no pārsūdzību un sūdzību izskatīšanas;

7.13.1.4. kādas pārbaudes tiek veiktas sūdzību izskatīšanas procedūras laikā;

7.13.1.5. kādas ir sūdzības izskatīšanas procesā iesaistīto pušu uzklaušanās iespējas;

7.13.1.6. procesuālās darbības, kas jāveic pēc sūdzību izskatīšanas procedūras;

7.13.1.7. kārtību, kādā un kam jānosūta apstiprinājums par sūdzības atbilstību un atbilstošiem sūdzības izskatīšanas termiņiem;

7.13.1.8. kārtība, kādā nosaka termiņus sūdzību izskatīšanas procesā.

8. VADĪBAS SISTĒMAS PRASĪBAS

8.1. Sertifikācijas struktūra nosaka un Inspekcijai iesniedz procedūras šādu procesu īstenošanai:

8.1.1. sertifikācijas kritēriju pārvaldības un apstiprināšanas process;

8.1.2. Sertifikācijas struktūras iekšējo procesu uzraudzība, kontrole, novērtēšana, atjaunināšana un uzlabošana;

8.1.3. sūdzību izskatīšanas vadība;

8.1.4. rīcība sertifikācijas un tās pamatojuma dokumentācijas apturēšanai un atsaukšanai;

8.1.5. sertifikācijas līgumu pārvaldība;

8.1.6. neatkarības nodrošināšana (objektivitāte/finansiālā stabilitāte) un attiecīgo pierādījumu pārvaldība;

8.1.7. sertifikācijas kritēriju/sertifikācijas lēmumu publicēšana;

8.1.8. resursu (cilvēkresursu un ārējo resursu) administrēšana;

8.1.9. pieteikumu administrēšanas kārtība;

8.1.10. sertifikācijas izmaiņu un sertifikātu izmantošanas uzraudzība;

8.1.11. novērtēšanas metožu atjaunināšanas vadība, kurā paredz, kā mainoties tiesiskajam regulējumam vai riska iestāšanās gadījumā, tiek nodrošināta atbilstība aktuālajam nepieciešamo tehnisko un organizatorisko pasākumu aizsardzības līmenim;

8.1.12. kontroles pasākumi, lai nodrošinātu vērtēšanas metožu dokumentēšanu un novērtēšanu;

8.1.13. attiecināmo tiesiskā regulējuma izmaiņu apzināšana un ieviešana procesos (procedūrās);

8.1.14. Klienta un sertifikācijas struktūras līguma sastāvdaļu noteikšana;

8.1.15. potenciālo risku un ievainojamības uzskaitē, tostarp informācijas tehnoloģijās, ierīcēs un drošības tehnoloģijās;

8.1.16. tehnoloģiju attīstības ietekme uz apstrādes darbībām, tehnisko un organizatorisko pasākumu uzraudzību.

8.1.17. izmaiņu noteikšana Inspekcijas un EDAK prasībās attiecībā uz kritērijiem un sertifikācijas shēmām, un noteiktas procedūras, kā šīs izmaiņas nekavējoties tiek integrētas sertifikācijas struktūras procesos. Sertifikācijas struktūrai jābūt ieviestām iekšējām procedūrām, lai informētu Inspekciju par visām veiktajām izmaiņām.

8.2. Lai nodrošinātu saziņu starp LATAK, Inspekciju, sertifikācijas struktūru un Klientu, sertifikācijas struktūra veic:

8.2.1. Sertifikācijas struktūras dokumentu uzskaiti, tostarp:

8.2.1.1. informācijas pieprasījumi un atbildes uz tiem;

8.2.1.2. sūdzības un atbildes uz tām.

8.2.2. Pieteikuma izskatīšanas procesa dokumentu, tostarp informācijas par pieteikuma statusu, uzskaiti;

8.3. Sertifikācijas institūcija nodrošina sertifikācijas procesa dokumentu uzglabāšanu trīs gadus, kamēr sertifikācija ir spēkā, kā arī vēl vienu gadu pēc sertifikācijas līguma termiņa beigām. Ja rodas strīds starp sertifikācijas iestādi, Klientu, Inspekciju, dokumentu glabāšanas laiks var pārsniegt noteikto glabāšanas laiku uz laiku, kas nepieciešams strīda atrisināšanai.

8.4. Šiem pārvaldības principiem un to dokumentētai īstenošanai jābūt pārredzamiem, un sertifikācijas struktūra tos dara zināmus akreditācijas procesā un pēc Inspekcijas pieprasījuma jebkurā izmeklēšanas laikā datu aizsardzības pārskatīšanas vai sertifikācijas pārskatīšanas veidā.¹⁰

9. PIENĀKUMI UN KOMPETENCE

9.1. Novērtēšanas metožu atjaunināšana

Sertifikācijas struktūra nosaka un iesniedz Inspekcijai procedūru pieteikumu novērtēšanas metožu atjaunināšanai. Nepieciešamās izmaiņas ir jādokumentē, saglabājot dokumentu iepriekšējās versijas.

9.2. Zināšanu līmeņa uzturēšana

Sertifikācijas struktūra izstrādā un iesniedz procedūras, ar ko nodrošina savu darbinieku apmācību, lai atjauninātu viņu prasmes, mainoties tiesiskajam regulējumam, attiecīgajam(-ajiem) riskam(-iem), jaunākajiem tehnoloģijas sasniegumiem un tehnisko un organizatorisko pasākumu īstenošanas izmaksām.

9.3. Saziņa starp sertifikācijas struktūru un tās klientiem

9.3.1. Sertifikācijas struktūra izveido un iesniedz Inspekcijai procedūru saziņai ar Klientu, kas aptver:

9.3.1.1. dokumentus, kas attiecas uz akreditētās sertifikācijas struktūras uzdevumiem un pienākumiem, lai:

9.3.1.1.1. apstrādātu saņemtos un nosūtītos informācijas pieprasījumus;

9.3.1.1.2. nodrošinātu saziņu gadījumā, ja tiek iesniegta sūdzība par sertifikāciju;

9.3.1.1.3. nodrošinātu, ka par izmaiņām tiesiskajā regulējumā, kas attiecas uz turpmāku sertifikācijas procesu un tā uzraudzību, sertifikācijas struktūra nekavējoties paziņo Klientam;

9.3.1.2. sertifikācijas pieteikuma iesniegšanas un apstrādes kārtību, lai:

9.3.1.2.1. paziņotu par novērtēšanas gaitu un rezultātiem;

¹⁰ Datu regulas 42. panta 7. punkts, 58. panta 1. punkta b) apakšpunkts un 58. panta 1. punkta c) apakšpunkts

9.3.1.2.2. Klientu informētu gadījumā, ja tiek pieņemts lēmums nepiešķirt sertifikātu. Sertifikācijas institūcijai (struktūrai) ir pienākums Klientam skaidrot tā tiesības un kārtību, apstrīdot sertifikācijas institūcijas lēmumu;

9.3.1.2.3. kārtību, kādos gadījumos un kādā veidā Klients sniedz sertifikācijas struktūrai informāciju (Klienta izraisītu izmaiņu gadījumā).

9.4. *Novērtēšanas darbību dokumentēšana*

9.4.1. Sertifikācijas struktūrai ir jādokumentē tās veiktās sertifikācijas darbības. Pēc dokumentu atjaunināšanas jāreģistrē dokumenta versija un atjaunināšanas datums. Dokumentu iepriekšējās versijas jāglabā 3 gadus no grozījumu izdarīšanas dienas. Procedūru, kas nosaka novērtēšanas darbību dokumentēšanu, iesniedz Inspekcijai.

9.4.2. Sertifikācijas struktūra nosaka un Inspekcijai iesniedz procedūru informācijas sniegšanai Inspekcijai, kas aptver:

9.4.2.1. atbilstību 7.6.2. un 7.6.3. punktā ("*sertifikācijas lēmums*") noteiktajām prasībām, paziņojumus par saņemtajiem sertifikācijas pieteikumiem un/vai pieņemamo lēmumu izdot sertifikātu.

9.4.2.2. paziņojumus par sertifikāta izdošanas vai atsaukšanas iemesliem;¹¹

9.4.2.3. sertifikācijas procesa laikā konstatētiem datu aizsardzības pārkāpumiem;

9.4.2.4. sertifikācijas struktūra nodrošina un pēc Inspekcijas pieprasījuma izsniedz statistiku par pabeigtajiem un pārtrauktajiem sertifikācijas procesiem;

9.4.2.5. paziņojumus par visiem grozījumiem dokumentos, kas attiecas uz sertifikācijas pakalpojumu sniegšanu un kas sniegti brīdī, kad tiek novērtēta atbilstība akreditācijas prasībām, un šādu grozījumu iemeslus.

9.4.3. Sertifikācijas struktūra sadarbojas ar Inspekciju, sniedz Inspekcijai pieprasīto informāciju, ļauj tai veikt pārbaudes un/vai revīzijas.

9.5. *Sūdzību izskatīšanas administrēšana*

9.5.1. Sertifikācijas struktūras sūdzību izskatīšanas un pārsūdzēšanas procedūru nosaka kā pārvaldības sistēmas neatņemamu sastāvdaļu. Inspekcijai iesniedz procedūras aprakstu, kas tostarp paredz 9.5.2. punktā noteiktās prasības izpildi.

9.5.2. Sertifikācijas institūcija Inspekcijai sniedz informāciju par pamatotām sūdzībām, ko saņēmusi sertifikācijas struktūra.

9.6. *Akreditācijas apturēšanas pārvaldība*

Sertifikācijas struktūra nosaka darbības, kas jāveic, ja tiek apturēta sertifikācijas struktūras akreditācija, piemēram, kā pārvaldības sistēmā tiek informēti sertifikācijas struktūras klienti (sertificējamās struktūras), un iesniedz izstrādāto kārtību Inspekcijai.

~~Lai nodrošinātu vienlīdzīgu, taisnīgu un pārredzamu pieeju administratīvo naudas sodu piemērošanā, Datu valsts inspekcija (Inspekcija) ir ieviesusi jaunu naudas soda aprēķina metodi, kas balstīta uz Eiropas Datu aizsardzības kolēģijas (EDAK) vadlīnijām Nr. 04/2022¹². Šī metode aizvieto iepriekšējo pieeju un sniedz uzņēmumiem skaidrību par to, kā tiek aprēķināti sodi par personas datu aizsardzības pārkāpumiem~~

¹¹ Datu regulas 43. panta 5. punkts

¹² ~~Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 04/2022 administratīvo naudas sodu aprēķināšanai saskaņā ar Vispārīgo datu aizsardzības regulu. Pieņemtas 2023. gada 24. maijā, pieejamas vietnē: https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_lv_0.pdf.~~

Piemērojamā naudas soda apmērs tiek noteikts divos posmos:

- **1. posms — sākumpunkta (sākotnējās summas) noteikšana atkarībā no pārkāpuma smaguma;**
- **2. posms — piemērojamā naudas soda noteikšana atkarībā no apgrozījuma, ņemot vērā pārējos apstākļus.**

1. Sākumpunkta (sākotnējās summas) noteikšana atkarībā no pārkāpuma smaguma

Pirmajā posmā tiek veikts pārkāpuma smaguma izvērtējums un soda sākumpunkta (sākotnējās summas) noteikšana, kas ir pamats turpmākajam soda aprēķinam.

Inspekcija izmanto tās izstrādāto punktu skalu, lai izvērtētu kritērijus, pēc kuriem tiek noteikts pārkāpuma smagums un attiecīgi naudas soda sākumpunkts, proti, sākotnējā summa.

1.1. Pārkāpuma smaguma izvērtējums

Izmantojot punktu skalu, tiek analizēti Datu regulā noteiktie kritēriji, piemēram, pārkāpuma būtība, skarto datu subjektu skaits, nodarītais kaitējums, pārkāpuma ilgums u.c. Katram kritērijam tiek piešķirts atbilstošs punktu skaits noteiktā amplitūdā, kas kopsummā norāda uz pārkāpuma smaguma pakāpi. Šajā posmā analizētie kritēriji (ja tie ir piemērojami un nosakāmi konkrētās lietas apstākļiem) ir šādi:

- **Pārkāpuma raksturs un būtība** — cik būtiski pārkāpums ir aizskāris datu subjektu intereses vai tiesības;
- **Apstrādes veids un apjoms** — vai apstrāde ir vietēja, valsts mēroga vai pārrobežu;
- **Datu apstrādes nolūks** — vai datu apstrāde ietilpst pārzīņā “pamatdarbībās”;
- **Skarto datu subjektu skaits** — jo vairāk cilvēku ietekmējis pārkāpums, jo smagāks tas ir;
- **Kaitējuma apmērs** — vai ir radīts reāls vai konstatējams potenciāls kaitējums;
- **Pārkāpuma ilgums** — ilgstoši pārkāpumi tiek vērtēti kā smagāki;
- **Pārkāpuma tišs vai netišs raksturs** — tiša, apzināta rīcība palielina pārkāpuma smagumu;
- **Skarto datu kategorijas** — īpaši aizsargājami dati (piemēram, veselības, bērnu dati) palielina smagumu.

Atbilstoši kopsummā iegūtajam punktu skaitam pārkāpums tiek klasificēts **kā maznozīmīgs (viegls), vidēji smags vai smags**, un tiek noteikts sākotnējais soda diapazons.

1.2. Sākumpunkta (sākotnējās summas) noteikšana

Kad noteikts pārkāpuma smagums, pamatojoties uz algoritma aprēķināto diapazonu, tiek noteikts attiecīgs soda sākumpunkts (sākotnējā summa) atkarībā no Datu regulas pārkāpuma veida, piemēram:

- **maznozīmīgs pārkāpums:** līdz 1 vai 2 milj. EUR, ja gada apgrozījums ir mazāks par 500 milj. EUR, atkarībā no tā, kurš Datu regulas 83. panta 4. 6. punkts piemērojams;
- **vidēji smags pārkāpums:** līdz 2 vai 4 milj. EUR, ja gada apgrozījums ir mazāks par 500 milj. EUR, atkarībā no tā, kurš Datu regulas 83. panta 4. 6. punkts piemērojams;
- **smags pārkāpums:** līdz 10 vai 20 milj. EUR, ja gada apgrozījums ir mazāks par 500 milj. EUR, atkarībā no tā, kurš Datu regulas 83. panta 4. 6. punkts piemērojams.

2. Piemērojamā naudas soda noteikšana atkarībā no apgrozījuma, ņemot vērā pārējos apstākļus

Soda aprēķina otrajam posmam ir būtiska nozīme, jo tas nodrošina, ka sods ir samērīgs, efektīvs un pietiekami stingrs, lai uzņēmumus motivētu ievērot Datu regulas prasības. Proti, pirmajā posmā tiek noteikts pārkāpuma smagums un soda sākumpunkts (sākotnējā summa), taču tas vēl nenosaka konkrēto rezultātā

~~piemērojamo soda apmēru. Tāpēc otrajā posmā tiek veikts soda summas precīzs aprēķins, ņemot vērā uzņēmuma finansiālo kapacitāti un lietas individuālos apstākļus.~~

~~Šajā posmā sākotnējā summa tiek koriģēta atbilstoši uzņēmuma apgrozījumam, lai nodrošinātu, ka sods ir proporcionāls uzņēmuma lielumam un spējai to samaksāt. Šī korekcija ir īpaši svarīga, lai novērstu situācijas, kad vienāds piemērotais sods mazam uzņēmumam būtu finansiāli graujošs, bet lielam — nebūtisks.~~

~~Visbeidzot, tiek izvērtēti atbildību mīkstinoši un pastiprinoši apstākļi, kas ļauj pielāgot soda apmēru konkrētās lietas kontekstā. Mīkstinoši apstākļi, piemēram, pārkāpuma efektīva un tūlītēja novēršana, sadarbība ar Inspekciju, pārkāpuma un rīcības nožēlošana var samazināt sodu. Savukārt pastiprinoši apstākļi, piemēram, tiša rīcība, iepriekšēji pārkāpumi, sistemātiska personas datu aizsardzības prasību neievērošana vai sadarbības trūkums, var to palielināt.~~

2.1. Summas korekcija, pamatojoties uz apgrozījumu un papildu apstākļiem

~~Šajā posmā sākotnējā summa tiek pielāgota jeb koriģēta, ņemot vērā:~~

- ~~• **Uzņēmuma apgrozījumu** — jo lielāks apgrozījums, jo lielāks piemērotais sods (piemēram, uzņēmumiem ar apgrozījumu līdz 2 milj. EUR summas korekcija paredz sodu 0,2–0,4 % apmērā no sākotnējās summas, bet uzņēmumiem ar apgrozījumu 250–500 milj. EUR summas korekcija paredz sodu 40–100 % apmērā no sākotnējās summas);~~
- ~~• **Atbildību mīkstinošus vai pastiprinošus apstākļus.** Šie lietas apstākļi var samazināt vai palielināt soda apmēru, nodrošinot taisnīgu pieeju katrā lietā, lai nodrošinātu, ka sods ir iedarbīgs, samērīgs un atturošs, kā to paredz Datu regulas 83. pants.~~

2.2. Piemērojamā naudas soda apmēra noteikšana

~~Pēc sākotnējās summas korekcijas tiek noteikta galīgā lietā piemērojamā naudas soda summa, kas atbilst Datu regulas 83. panta prasībām:~~

- ~~• **iedarbīga** — soda mērķis ir pārtraukt un novērst turpmākus pārkāpumus;~~
- ~~• **samērīga** — sods atbilst pārkāpuma smagumam un uzņēmuma kapacitātei;~~
- ~~• **atturoša** — sods kalpo kā brīdinājums arī citiem pārzinīem (uzņēmumiem).~~

~~Galīgā naudas soda summa tiek apstiprināta, pamatojoties uz visiem izvērtētajiem kritērijiem, un tiek norādīta Inspekcijas lēmumā. Tādējādi tiek nodrošināts, ka uzliktais sods nav tikai matemātisks rezultāts, bet gan taisnīgs un lietas kontekstam atbilstoši pieņemts lēmums, kura izvērtēšanā tiek ņemta vērā gan pārkāpuma būtība, gan uzņēmuma vai fiziskās personas finansiālie apstākļi un situācija.~~

~~**Kopumā šī metode ļauj Inspekcijai objektīvi un konsekventi noteikt un piemērot naudas sodus par konstatētajiem pārkāpumiem, vienlaikus ņemot vērā katras lietas individuālos apstākļus.**~~