

ZIŅOJUMS

**PAR VISPĀRĪGĀS DATU AIZSARDZĪBAS REGULAS PRASĪBU
IZPILDI VALSTS UN PAŠVALDĪBU IESTĀDĒS ATTIECĪBĀ UZ
DATU AIZSARDZĪBAS SPECIĀLISTA AMATU**

Šī ziņojuma mērķis ir informēt par Datu valsts inspekcijas veiktās pārbaudes rezultātiem, secinājumiem un priekšlikumiem par Vispārīgās datu aizsardzības regulas prasību izpildi valsts un pašvaldību iestādēs attiecībā uz datu aizsardzības speciālista norīkošanu, kā arī tā prasību izpildi saistībā ar datu aizsardzības speciālista amatu valsts un pašvaldības iestādēs.

Lietotie saīsinājumi:

Inspekcija	Datu valsts inspekcija
FPDAL	Fizisko personu datu apstrādes likums
Iestādes	Valsts un pašvaldību iestādes
Datu regula	Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 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)

1. VISPĀRĪGĀ INFORMĀCIJA

1.1. Preventīvā pārbaude Valsts pārvaldē fizisko personu datu aizsardzības jomā

Īstenojot Datu regulā un Datu likumā noteiktos uzdevumus un tiesības datu aizsardzības jomā, Inspekcija, atbilstoši savai kompetencei un uzdevumiem, kas noteikti Datu regulas 57. pantā un Datu likuma 4. pantā, 2022. gada 22. decembrī uzsāka preventīvo pārbaudi Iestādēs par Datu regulas prasību izpildi attiecībā uz datu aizsardzības speciālista amata atbilstību Datu regulas prasībām.

Inspekcija, preventīvās pārbaudes ietvaros, vērtēja vai Iestāžu ieceltais datu aizsardzības speciālists ir iekļauts Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā atbilstoši Datu likuma 18. pantam. Tika vērtēti Iestāžu ieceltie datu aizsardzības speciālisti, kas ir nodarbināti uz darba līguma pamata, to daudzums un attiecība pret Iestāžu norīkotajiem datu aizsardzības speciālistiem, kas ir piesaistīti kā ārpalpojums. Tostarp, piesaistītajiem datu aizsardzības

speciālistiem, kas ir piesaistīti kā ārpalpojums, tika vērtēta līgumā norādītā informācija, kurā noteikta datu aizsardzības speciālista uzdevumu izpilde. Tāpat tika vērtēts, kādi kritēriji tika ņemti vērā ieceļot datu aizsardzības speciālistu un tas vai tika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā. Tika vērtēts arī kā Iestādes īsteno pienākumu nodrošināt to, ka ieceltajam datu aizsardzības speciālistam ir pietiekošs kvalifikācijas un speciālo zināšanu līmenis, lai pildītu pienākumus. Tika vērtēts vai Iestādēs tiek nodrošināts, ka datu aizsardzības speciālists tiek laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību un kā tas tiek nodrošināts. Tāpat tika vērtēts kā tiek nodrošināta datu aizsardzības speciālista neatkarība (spēja neatkarīgi pildīt savus pienākumus un uzdevumus) un vai ieceļot datu aizsardzības speciālistu, tika vērtēta interešu konflikta iespējamība un pakļautība un procesi, kas to novērstu. Piemēram, iekšējo noteikumu izstrāde, lai novērstu interešu konfliktu iespējamību un ietekmi uz datu aizsardzības speciālistu, ievērojot pakļautības formu, kā arī citi pasākumi, kas novērstu vai mazinātu interešu konfliktu iespējamību. Pārbaudes gaitā tika vērtēts arī resursu apjoms, kas tika sniegts no pārziņa puses datu aizsardzības speciālistam, lai viņš pilnvērtīgi spētu veikt savus amata pienākumus. Papildus iepriekš minētajam tika vērtēta Iestāžu privātuma politika un korelācija ar datu aizsardzības speciālista iesaisti privātuma politikas veidošanā.

Procesuālās darbības preventīvās pārbaudes ietvaros par Datu regulas prasību izpildi Iestādēs attiecībā uz datu aizsardzības specialista norīkošanu un prasību izpildi Iestādēs īstenoja Inspekcijas Preventijas nodaļa.

1.2. Pārbaudīto Iestāžu atlase.

Pārbaudē iekļauto Iestāžu atlase tika veikta Iestādēm, kuru veiktās darbības ar personas datiem ietilpst Datu regulas tvērumā, kuru personas datu apstrādes uzraudzību nodrošina Inspekcija.

Ievērojot Inspekcijas Datu regulā un FPDAL noteikto kompetenci, Preventīvās pārbaudes rezultātā tika uzsāktas pārbaudes un nosūtītas vēstules 129 iestādēm.

2. DATU AIZSARDZĪBAS SPECIĀLISTS IESTĀDĒS

Datu aizsardzības speciālists ir persona ar speciālām zināšanām datu aizsardzības tiesību un praktiskas datu aizsardzības piemērošanā. Līdzīgi kā darba drošības speciālists, kam ir speciālas zināšanas darba aizsardzības sistēmas organizācijā un nepieciešamo prasību

nodrošināšanā attiecībā uz darba drošību, tā arī datu aizsardzības speciālists ir eksperts ar speciālām zināšanām savā atbildības jomā.

Datu aizsardzības speciālists ir konkrētās organizācijas vadības palīgs lēmumu pieņemšanā jautājumos, kas saistīti ar personas datu apstrādi un aizsardzību. Tā galvenā funkcija ir, izmantojot savas speciālās zināšanas, sniegt neatkarīgu viedokli par organizācijas plānoto vai jau ieviesto personas datu apstrādes procesu atbilstību Datu regulai un citiem saistošiem normatīvajiem aktiem.

Par labu praksi ir atzīstama datu aizsardzības speciālista iesaiste no organizācijas vadības puses jebkurā procesā, kurā organizācija plāno apstrādāt (vai jau apstrādā) personas datus.

Neatkarīgi no datu aizsardzības speciālista sniegtajiem ieteikumiem, atbildīga par personas datu apstrādi un ar to saistītiem jautājumiem būs organizācija, kas speciālistu piesaistījusi. Datu aizsardzības speciālista amats nevar tikt apdraudēts gadījumos, ja datu aizsardzības prasības netika izpildītas, bet no šī speciālista tika saņemti ieteikumi, tāpat kā gadījumos, ja datu aizsardzības speciālists netika iesaistīts svarīgos datu apstrādes jautājumos.

Piemēram, datu aizsardzības speciālists būtu piesaistāms, lai novērtētu organizācijas iekšējās kārtības lietvedības apriti; jaunas tīmekļa vietnes izstrādi; mārketinga stratēģijas izveidi, ja tajās plānots izmantot identificētu vai identificējamu fizisko personu datus. Savukārt izstrādāt pašus dokumentus (lietvedības organizēšanas kārtība, tīmekļa vietnes tehniskā specifikācija u.tml.) datu aizsardzības speciālistam nedrīkstētu uzdot – tas ne tikai radītu interešu konfliktu (jo datu aizsardzības speciālistam būtu jāvērtē sava paveiktā darba kvalitāte), bet arī pazeminātu speciālista sniegtā pakalpojuma kvalitāti, jo izpaliktu jomas eksperta veikta izstrādātā dokumenta kvalitātes pēckontrole.

Visām publiskajām iestādēm vai struktūrām, izņemot tiesas, saskaņā ar Datu regulas 37.panta 1. punkta a) apakšpunktu ir pienākums iecelt datu aizsardzības speciālistu un ievērot visas Datu regulas 38. pantā noteiktās prasības Datu aizsardzības speciālista statusa nodrošināšanai.

Saskaņā ar Datu regulas 37. panta 3. punktu vienu datu aizsardzības speciālistu var iecelt vairākām publiskām iestādēm vai struktūrām, ņemot vērā to organizatorisko struktūru un izmēru. Tie paši apsvērumi attiecas uz līdzekļiem un saziņu. Ņemot vērā, ka datu aizsardzības speciālists ir atbildīgs par dažādiem uzdevumiem, pārzinis vai apstrādātājs nodrošina, ka viens datu aizsardzības speciālists pēc nepieciešamības ar komandas palīdzību var veikt šos uzdevumus efektīvi, neraugoties uz to, ka viņš ir iecelts vairākām publiskām iestādēm un struktūrām.

Datu aizsardzības speciālistu “ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā un spēju pildīt 39. pantā minētos uzdevumus”. Nepieciešamais speciālo zināšanu līmenis būtu jānosaka saskaņā ar veiktajām datu apstrādes darbībām un aizsardzību, kas nepieciešama apstrādājamiem personas datiem.

2.1. Nepieciešamais speciālo zināšanu līmenis

Nepieciešamais speciālo zināšanu līmenis nav precīzi noteikts, bet tam ir jābūt atbilstošam datu un organizatorisko procesu sensitivitātei, sarežģītībai un apjomam. Piemēram, ja datu apstrādes darbība ir īpaši sarežģīta vai ir iesaistīts liels sensitīvu datu apjoms, datu aizsardzības speciālists var būt nepieciešama lielāka specializācijas un atbalsta pakāpe. Tāpat, ja Iestādei plānota jauna, specifiska vai īpaši sensitīva/sarežģīta apstrāde, ja tas nepieciešams datu aizsardzības speciālista pienākumu kvalitatīvai veikšanai, Iestādei būtu jāpaaugstina datu aizsardzības speciālista speciālo zināšanu līmenis atbilstoši plānotajai apstrādes specifikai/sensivitātei.

2.2. Profesionālā kvalifikācija.

Lai arī Datu regulā nav noteikta profesionālā kvalifikācija, kas jāņem vērā, ieceļot datu aizsardzības speciālistu, tas ir būtisks nosacījums, lai datu aizsardzības speciālists pārzinātu datu aizsardzības tiesisko regulējumu, praksi, kā arī padziļināti izprastu Datu regulu.

2.3. Spēja veikt pienākumus

Spēja veikt datu aizsardzības speciālista pienākumus ir skaidrojama kā tāda, kas attiecas gan uz personisko kvalifikāciju un zināšanām, gan arī uz to statusu organizācijā. Personiskajai kvalifikācijai ir jāietver, piemēram, integritāte un augsta profesionālā ētika. Datu regulas noteikumu izpildes nodrošināšanai ir jābūt datu aizsardzības speciālista galvenajām rūpēm. Datu aizsardzības speciālistam ir galvenā nozīme datu aizsardzības kultūras veicināšanā organizācijā, un tas palīdz īstenot būtiskus Datu regulas elementus, piemēram, datu apstrādes principus, datu subjektu tiesības, integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, apstrādes darbību uzskaiti, apstrādes drošību un datu aizsardzības pārkāpumu paziņošanu un informēšanu par to.

2.4. Datu aizsardzības speciālista darbība saskaņā ar līgumu

Datu aizsardzības speciālista funkcijas var veikt arī saskaņā ar pakalpojumu līgumu, kas noslēgts ar individu vai organizāciju, kas neietilpst pārziņa/apstrādātāja organizācijā. Pēdējā gadījumā ir svarīgi, lai visi organizācijas dalībnieki, kas veic datu aizsardzības speciālista funkcijas, izpilda visas piemērojamās Datu regulas 4.iedaļas prasības (piem., lai nevienam nerastos interešu konflikts). Tikpat svarīgi ir, lai katru šādu dalībnieku pasargā Datu regulas noteikumi (piem., nedrīkst nepamatoti pārtraukt darba attiecības ar datu aizsardzības speciālistu, taču nedrīkst arī nepamatoti atlaist organizācijas atsevišķus dalībniekus, kas veic datu aizsardzības speciālista uzdevumus). Vienlaikus var apvienot individuālas spējas un stiprās puses, lai vairāki indivīdi, kuri strādā komandā, varētu efektīvāk apkalpot klientus.

2.5. Normatīvais ietvars

Datu regulas 37. pants. (Datu aizsardzības speciālista iecelšana).

Datu regulas 38. pants. (Datu aizsardzības speciālista statuss).

Datu regulas 39. pants. (Datu aizsardzības speciālista uzdevumi).

3. KOPSAVILKUMS

Lai izvērtētu preventīvās pārbaudes ietvaros Datu regulas prasību izpildi attiecībā uz datu aizsardzības speciālista norīkošanu atbilstību Datu regulas prasībām Iestādēs, Inspekcija lūdzta Iestādēm sniegt sekojošu informāciju:

1. Vai Iestādei pēdējā gada laikā ir mainījies datu aizsardzības speciālists;
 - 1.1. Ja jā, lūdzam iesniegt informāciju par iecelto datu aizsardzības speciālistu (vārds, uzvārds, tālruna numurs, elektroniskā pasta vēstule).;
 - 1.1.2. Vai ieceltais datu aizsardzības speciālists ir iekļauts Datu valsts inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā atbilstoši Datu likuma 18.pantam
 - 1.2. Vai ieceltais datu aizsardzības speciālists ir nodarbināts uz darba līguma pamata vai arī tas ir piesaistīts kā ārpalpojums;
 - 1.2.1. Ja datu aizsardzības speciālista pakalpojumus sniedz ārpalpojuma sniedzēji, lūdzam iesniegt līguma kopiju vai tā izrakstu, kurā noteikta datu aizsardzības speciālista uzdevumu izpilde;
2. Vai ieceļot datu aizsardzības speciālistu, tika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā;
 - 2.1. Ja jā, kādi kritēriji tika vērtēti un ņemti vērā;
 - 2.2. Ja nē, lūdzam sniegt skaidrojumu kāpēc netika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā;
 - 2.3. Kā tiek nodrošināts, ka datu aizsardzības speciālistam ir pietiekošs kvalifikācijas un speciālo zināšanu līmenis, lai pildītu pienākumus;
3. Vai tiek nodrošināts, ka datu aizsardzības speciālists tiek laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību;
4. Kā tiek nodrošināta datu aizsardzības speciālista neatkarība (spēja neatkarīgi pildīt savus pienākumus un uzdevumus);
 - 4.1 Vai ieceļot datu aizsardzības speciālistu, tika vērtēta interešu konflikta iespējamība un pakļautība;
 - 4.2. Vai ir izstrādāti iekšējie noteikumi, lai novērstu interešu konfliktu iespējamību un ietekmi uz datu aizsardzības speciālistu, ievērojot pakļautības formu;
 - 4.3. Vai tika ieviesti citi pasākumi, lai novērstu interešu konfliktu iespējamību;
5. Kādi resursi (tehniskais aprīkojums, piekļuve pārziņa apstrādes procesiem un/vai personas datus saturošām sistēmām) no pārziņa puses tiek sniegti datu aizsardzības speciālistam lai viņš spētu veikt savus amata pienākumus;

6. Papildus iepriekš minētajam lūdzam iesniegt saiti uz tīmekļa vietnes sadaļu, kur ir atrodama privātuma politika;

6.1. Lūzdu sniegt informāciju vai politikas izstrādē tika iesaistīts datu aizsardzības speciālists;

6.2. Vai datu aizsardzības speciālists ir sniedzis viedokli par privātuma politiku

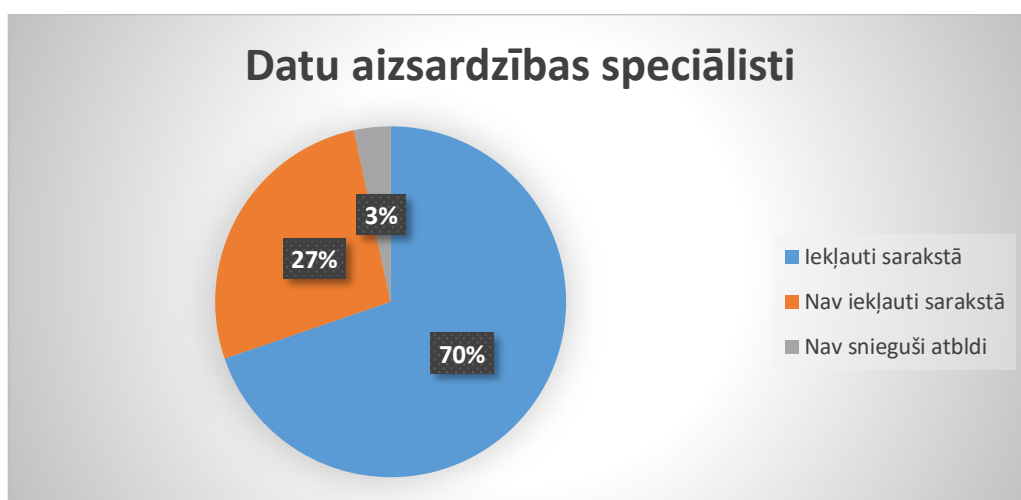
6.3. Vai datu aizsardzības speciālista viedoklis ir ņemts vērā;

Inspekcija lūdza 129 Iestādēm līdz **2023. gada 10. februārim** sniegt informāciju par Datu regulas prasību izpildi saistībā ar datu aizsardzības institūtu. Uz 2023. gada 15. maiju atbildi Inspekcijai uz tās pieprasījumu ir sniegušas 119 Iestādes.

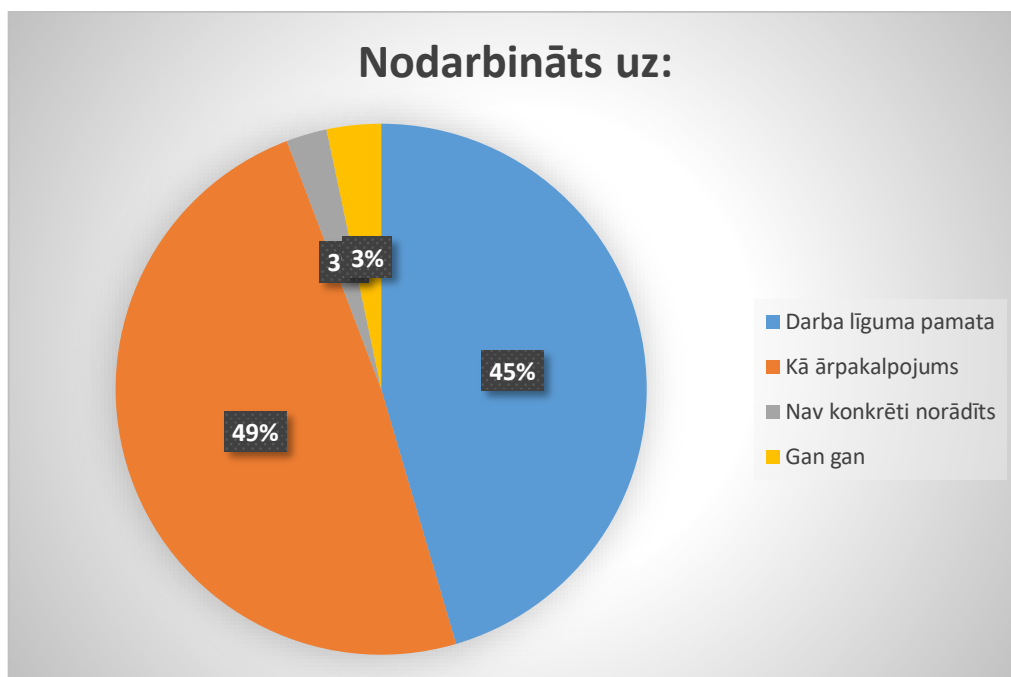
Ziņojumā sniegtā informācija par Preventīvās pārbaudes rezultātiem apkopota atbilstoši Iestāžu iesniegtajām atbildēm par datu aizsardzības speciālista atbilstību Datu regulas prasībām.

4. PĀRBAUDES REZULTĀTI

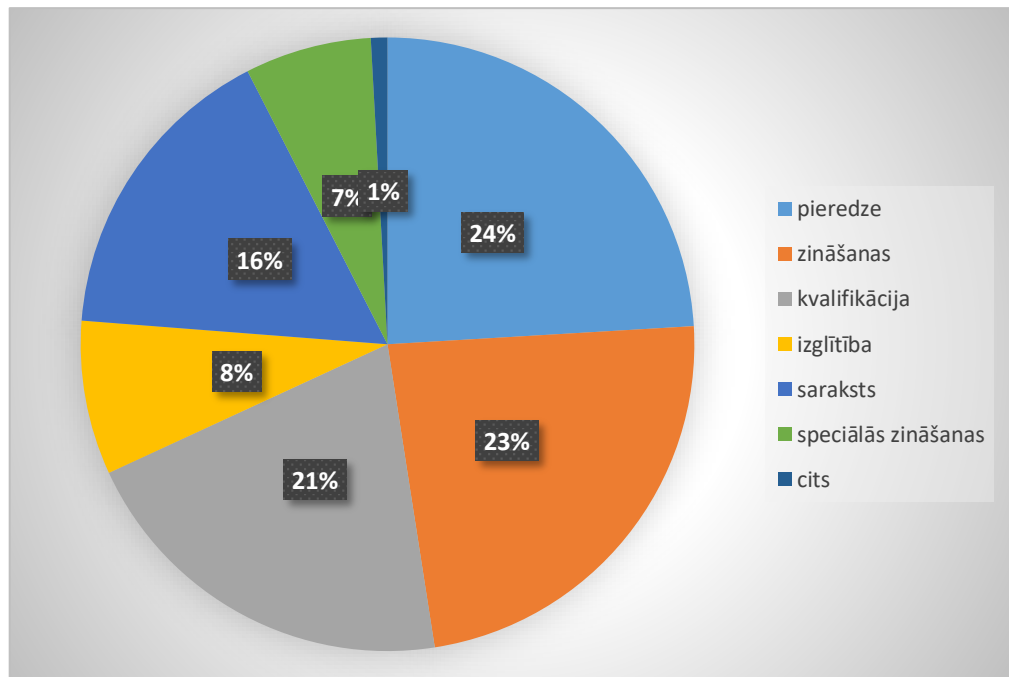
- Vērtējot pārbaudes ietvaros saņemtās Iestāžu atbildes, secināms, ka visām Iestādēm ir norīkots datu aizsardzības speciālists;
- 83 no ieceltajiem datu aizsardzības speciālistiem ir iekļauti Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā atbilstoši Datu likuma 18. pantam; 32 no ieceltajiem datu aizsardzības speciālistiem nav iekļauti Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā atbilstoši Datu likuma 18.pantam; 4 Iestādes nav sniegušas konkrētu vai saprotamu atbildi par to vai to ieceltais datu aizsardzības speciālistiem ir iekļauts Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā;



- 55 Iestādēm ieceltais datu aizsardzības speciālists ir nodarbināts uz darba līguma pamata, savukārt kā ārpalpojums tas ir piesaistīts 59 Iestādēm. 3 Iestādes nav sniegušas konkrētu atbildi uz šo jautājumu vai arī to atbilde nav bijusi saprotama. 4 Iestādes norādīja, ka ir piesaistīts datu aizsardzības speciālists gan uz darba līguma pamata, gan, kā ārpalpojums;



- 115 Iestādes atbildēja, ka ieceļot datu aizsardzības speciālistu, tika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā. 3 Iestādes norādīja, ka ieceļot datu aizsardzības speciālistu, netika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā. Savukārt viena Iestāde nav norādījusi informāciju par minēto;
- Iestādes, vērtēšanas laikā, ņēmušas vērā dažādus kritērijus. Visvairāk Iestādes ņēmušas vērā: pieredze (83 Iestādes); zināšanas (81 Iestāde); kvalifikācija (71 Iestāde); izglītība (28 Iestādes); saraksts (56 Iestādes; 4 Iestādes esamību sarakstā norādījušas kā vienīgo kritēriju, kas vērtēts); speciālās zināšanas (23 Iestādes); izpratne (1 Iestāde); apmeklētie kursi (1 Iestāde); Viena iestāde nav norādījusi atbildi uz šo jautājumu;



- Pienākumu nodrošināt, ka datu aizsardzības speciālistam ir pietiekošs kvalifikācijas un speciālo zināšanu līmenis, lai pildītu pienākumus Iestādes izpilda sekojoši: 72 Iestādes norīko tos uz apmācībām; 7 Iestādes vērtē to iesūtītos darbības pārskatus; 27 Iestādes norādījušas, ka datu aizsardzības speciālista sarakstā esamība nodrošina to, ka tam pietiekošs kvalifikācijas un speciālo zināšanu līmenis, lai pildītu pienākumus; 6 Iestādes norāda, ka datu aizsardzības speciālists ir pats par to atbildīgs; 7 iestādes nav norādījušas atbildi uz šo jautājumu.
- Prasība nodrošināt, ka datu aizsardzības speciālists tiek laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību tiek nodrošināta sekojoši: 31 Iestādei šī prasība atrunāta savstarpēji noslēgtajā līgumā; 52 Iestādes to ietvērušas iekšējajos noteikumos / kārtībā; 27 Iestādes to nodrošina iesaistot datu aizsardzības speciālistu visos procesos; 2 Iestādes norādījušas uz ārpakalpojuma elementu šī pienākuma nodrošināšanai; 2 Iestādes nav sniegušas atbildi uz šo jautājumu; 2 Iestādes lūdz sniegt viedokli dažādos jautājumos; 1 Iestāde norāda ka datu aizsardzības speciālists tiek iesaistīts sapulcēs; 1 Iestāde to nodrošina ar neierobežotu tel. konsultācijām un el. Saraksti ar datu aizsardzības speciālistu; 1 Iestāde norāda, ka šo prasību nodrošina sarakstā esamība;
- Nodrošinot datu aizsardzības speciālista neatkarību: 37 Iestādes šo prasību

ietvērūšas iekšējajos noteikumos / kārtībā; 23 Iestādēm šī prasība atrunāta savstarpēji noslēgtajā līgumā vai ietverts amata aprakstā; 49 Iestādes norādījušas uz ārpakalpojuma elementu šī pienākuma nodrošināšanai; 1 Iestādei ir izveidots atsevišķs amats; 4 Iestādes nav norādījušas atbildi uz šo jautājumu vai arī no atbildes nevar skaidri izsecināt to; 7 Iestādes norādījušas ka to nodrošina tiešā pakļautība vadītājam; 4 Iestādes norādīja, ka īsteno vairākus mehānismus šī pienākuma īstenošanai;

- Ieceļot datu aizsardzības speciālistu, 94 Iestādēs tika vērtēta interešu konflikta iespējamība un pakļautība; 7 Iestādēs šāda iespējamība netika vērtēta; 18 Iestādes nesniedza konkrētu atbildi uz šo jautājumu;
- Lai novērstu interešu konfliktu iespējamību un ietekmi uz datu aizsardzības speciālistu 43 Iestādes norādīja, ka tām ir izstrādāti atsevišķi iekšējie noteikumi vai prasības iestrādātas esošajos noteikumos; 54 Iestādes norādīja, ka tām nav izstrādāti iekšējie noteikumi vai iestrādātas prasības esošajos noteikumos; 22 Iestādes nesniedza atbildi uz šo jautājumu;
- 78 Iestādes norādīja ka nav ieviesti citi pasākumi, lai novērstu interešu konfliktu iespējamību, 13 Iestādes norādīja ka ir ieviesti citi papildus pasākumi, lai novērstu interešu konfliktu iespējamību. 28 Iestādes nesniedza atbildi uz šo jautājumu;
- Attiecībā uz sniegtajiem resursiem no pārziņa puses 47 Iestādes norādīja ka tika sniegti visi nepieciešamie resursi un informācija datu aizsardzības speciālistam, lai viņš spētu veikt savus amata pienākumus; 2 Iestādes norādīja, ka informācija un pārējie resursi tiek sniegti pēc pieprasījuma; 34 Iestādes norādīja ka tiek nodrošināta piekļuve sistēmām; 29 Iestādes norādīja ka tiek nodrošināta piekļuve procesiem; 2 Iestādes norādīja ka resursi netiek nodrošināti; 2 Iestādes norādīja ka nodrošina telpas, iekārtas un atbalstu, aprīkojumu; 3 Iestādēm nebija sniegta atbilde uz šo jautājumu vai arī atbilde nebija saprotama;



- 117 Iestādēm privātuma politikas izstrādē tika iesaistīts datu aizsardzības speciālists; 2 Iestādēm datu aizsardzības speciālists netika iesaistīts privātuma politikas izstrādē;
- Visas 117 Iestādes, kurām datu aizsardzības speciālists ir iesaistīts privātuma politikas izstrādē, norādīja, ka datu aizsardzības speciālists ir sniedzis viedokli par privātuma politiku;
- Visas 117 Iestādes norādīja, ka datu aizsardzības speciālista viedoklis ir ņemts vērā.

5. SECINĀJUMI

Secināms, ka absolūtais vairākums no ieceltajiem datu aizsardzības speciālistiem ir iekļauti Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā. Tas liecina par to, ka Iestādes vēlas nodrošināties attiecībā uz nepieciešamo zināšanu līmeni datu aizsardzības speciālistiem un dod priekšroku tiem, kas ir iekļauti Inspekcijas uzturētajā sarakstā. Savukārt tie ieceltie datu aizsardzības speciālisti, kas nav iekļauti Inspekcijas uzturētajā datu aizsardzības speciālistu sarakstā ir iecelti no Iestādes iekšējiem resursiem. Šādos gadījumos ir saskatāma korelācija ar Iestādes aktīvāku iesaisti datu aizsardzības speciālistu norīkošanai uz apmācībām, tādējādi datu aizsardzības speciālistam iegūstot vai paaugstinot nepieciešamās zināšanas.

Aptuveni pusei no Iestādēm ieceltais datu aizsardzības speciālists ir nodarbināts uz darba līguma pamata, kas nozīmē, ka aptuveni puse no Iestādēm iecelto datu aizsardzības

speciālistu ir izvēlējusies kā ārpalpojumu. Līdz ar to secināms, ka Iestādes izmanto dažādus mehānismus šo prasību izpildei.

Ņemot vērā, ka tiek izmantoti dažādi mehānismi datu aizsardzības speciālista institūta nodrošināšanai tiek izmantoti arī dažādi mehānismi lai izpildītu Datu regulas prasības. Iestādēm ar ārpalpojumu lielākoties prasības, kārtība, noteikumi, tiek atrunāti un iekļauti savstarpējā līgumā, savukārt Iestādēm, kurām ieceltais datu aizsardzības speciālists ir nodarbināts uz darba līguma pamata, Datu regulas prasības, lielākoties, tiek iekļautas iekšējo noteikumu sistēmā.

Kopumā Iestādes nodrošina nepieciešamos resursus datu aizsardzības speciālistam uzdevumu veikšanai, tomēr veidi kā tas tiek nodrošināts ir dažādi. Iespējams, saistīts ar iepriekšējā rindkopā secināto.

Faktiski visām Iestādēm politikas izstrādē tika iesaistīts datu aizsardzības speciālists. Savukārt tie, kam datu aizsardzības speciālists netika iesaistīts politikas izstrādē, norādīja, ka privātuma politika tika izstrādā jau iepriekš. Minētais nozīmē, ka Iestādes iesaista datu aizsardzības speciālistu savos iekšējajos procesos un to viedoklis tiek ņemts vērā. Kas savukārt liecina ka datu aizsardzības speciālista amats Iestādēs nostiprinās kā nozīmīgs instruments datu aizsardzības prasību izpildē un Iestādes atbilstības veicināšanā.

6. IETEIKUMI

Lai stiprinātu datu aizsardzības speciālista institūtu, nepieciešams veikt pasākumus Iestāžu izglītošanai par datu aizsardzības speciālista nepieciešamību, statusu, kompetencēm. Tāpat rosināms veikt izpēti par datu aizsardzības speciālista iecelšanas kritērijiem. Izpētes rezultātā veiktie secinājumi ļautu izprast noteicošos kritērijus datu aizsardzības speciālista izvēlē uz kā pamata, iespējams, varētu izstrādāt rekomendācijas/ieteikumus ar kritērijiem, kas palīdzētu Iestādei ar atbilstošākā datu aizsardzības speciālista izvēli.