

# ZIŅOJUMS

## PAR VISPĀRĪGĀS DATU AIZSARDZĪBAS REGULAS PRASĪBU IZPILDI ATTIECĪBĀ UZ DATU AIZSARDZĪBAS SPECIĀLISTA AMATU

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

Inspekcija	Datu valsts inspekcija
FPDAL	Fizisko personu datu apstrādes likums
organizācijas	Valsts, pašvaldību iestādes un asociācijas
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)
NIDA	Novērtējums par ietekmi uz datu aizsardzību
DS pieprasījums	Datu subjekta pieprasījums

### 1. VISPĀRĪGĀ INFORMĀCIJA

#### 1.1. Preventīvā pārbaude Valsts pārvaldē fizisko personu datu aizsardzības jomā

Eiropas Datu aizsardzības kolēģija (EDAK) 15. martā uzsāka koordinētu pārbaudi par datu aizsardzības speciālista institūtu. Visa gada garumā 26 uzraudzības iestādes visā Eiropas Ekonomikas zonā (EEZ) (tostarp Eiropas Datu aizsardzības uzraudzītājs) veica koordinētu uzraudzības pasākumu par datu aizsardzības speciālistu iecelšanas un amata pienākumu izpildes novērtējumu.

Datu aizsardzības speciālistiem, kā starpniekiem starp uzraudzības iestādēm, fiziskām personām un organizācijām, ir būtiska loma datu aizsardzības regulējošo tiesību aktu ievērošanas veicināšanā un datu subjektu tiesību efektīvas aizsardzības sekmēšanā.

Lai novērtētu, vai organizācijās datu aizsardzības speciālista amats atbilst Datu regulas 37.-39. pantā noteiktajam, kā arī lai apzinātu nepieciešamos resursus datu aizsardzības speciālista pienākumu izpildei, Inspekcija ministrijām, to padotības iestādēm un asociācijām nosūtīja Eiropas Datu aizsardzības kolēģijas (“EDB”) koordinētās darbības ietvaros sagatavotās aptaujas anketas attiecībā uz datu aizsardzības speciālista iecelšanu un amatu.

Inspekcija, koordinētās pārbaudes ietvaros, vērtēja organizāciju iecelto datu aizsardzības speciālistu kvalifikāciju, pieredzi datu aizsardzības jomā. Tika vērtēti organizāciju ieceltie datu aizsardzības speciālisti, kas ir nodarbināti uz darba līguma pamata, to daudzums un attiecība pret organizāciju norīkotajiem datu aizsardzības speciālistiem, kas ir piesaistīti kā ārpalpojums. Tāpat tika vērtēts, kādi kritēriji tika ņemti vērā iecelot datu aizsardzības speciālistu un tas vai tika vērtēta tā profesionālā kvalifikācija un speciālās zināšanas datu aizsardzības tiesību un prakses jomā. Tika vērtēts arī kā organizācijas īsteno pienākumu nodrošināt to, ka ieceltajam datu aizsardzības speciālistam ir pietiekošs kvalifikācijas un speciālo zināšanu līmenis, lai pildītu pienākumus. Tika vērtēts vai organizācijās 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 iecelot 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 citu 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 organizāciju privātuma politika un korelācija ar datu aizsardzības speciālista iesaisti privātuma politikas veidošanā.

Procesuālās darbības koordinētās pārbaudes ietvaros par Datu regulas prasību izpildi organizācijās attiecībā uz datu aizsardzības specialista norīkošanu un prasību izpildi organizācijās īstenoja Inspekcijas Prevenzijas nodaļa.

## **1.2. Pārbaudīto organizāciju atlase.**

Pārbaudē iekļauto organizāciju atlase tika veikta organizācijām, 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 saņemtas aptaujas anketas no 179 organizācijām.

## **2. DATU AIZSARDZĪBAS SPECIĀLISTS**

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 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.

Datu aizsardzības speciālistu var iecelt arī citos gadījumos kas nav iepriekš uzskaitīti. Ievērojot datu aizsardzības speciālista darbības specifiku, tā piesaiste jautājumam, kas saistīti ar personas datu aizsardzību, izlemšanā būtu uzskatāma par labo praksi un ir atbalstāma visos uzņēmumos, arī gadījumos, kad datu aizsardzības speciālista piesaiste organizācijā neizriet no saistoša normatīvā akta.

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 apstrādātajiem 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 organizācijai plānota jauna, specifiska vai īpaši sensitīva/sarežģīta apstrāde, ja tas nepieciešams datu aizsardzības speciālista pienākumu kvalitatīvai veikšanai, organizācijai būtu jāpaaugstina datu aizsardzības speciālista speciālo zināšanu līmenis atbilstoši plānotajai apstrādes specifikai/sensitivitātei.

## **2.2. Profesionālā kvalifikācija.**

Lai arī Datu regulā nav noteikta profesionālā kvalifikācija, kas jāņem vērā, iecelot 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

Inspekcija 2023. gada 4. jūlijā izsūtīja vēstuli ministrijām un asociācijām un lūdza līdz 2023. gada 14. augustam aizpildīt aptauju, kā arī pārsūtīt to un līdz 2023. gada 14. augustam lūgt aizpildīt savām padotības iestādēm / asociācijas dalībniekiem.

Nemot vērā minēto 179 organizācijas aizpildīja Eiropas Datu aizsardzības kolēģijas ekspertu grupas izstrādāto aptaujas anketu.

Lai izvērtētu koordinētās pārbaudes ietvaros Datu regulas prasību izpildi attiecībā uz datu aizsardzības speciālista norīkošanu atbilstību Datu regulas prasībām organizācijās, Inspekcija lūdza sniegt sekojošu informāciju:

1. Vai organizācija ir iecēlusi datu aizsardzības speciālistu, un, ja atbilde ir “jā”, uz kāda pamata?
2. Vai persona, kas iecelta par datu aizsardzības speciālistu, darbojas kā vienīgais datu aizsardzības speciālists uzņēmumu grupā vai vairākās iestādēs vai struktūrās?
3. Vai datu aizsardzības speciālists ir organizācijas darbinieks vai arī uzdevumi tiek pildīti, pamatojoties uz pakalpojumu līgumu?
4. Uz kādu termiņu datu aizsardzības speciālists ir iecelts amatā?
5. Kurā organizācijas departamentā/nodaļā ietilpst datu aizsardzības speciālists?
6. Kurā no turpmāk minētajām tēmām organizācijas datu aizsardzības speciālistam (vai tā darbiniekiem) ir pieredze vai zināšanas?
7. Kuri no turpmāk minētajiem faktoriem, ieceļot datu aizsardzības speciālistu, tika noteikti kā prasības amatam?
8. Cik gadu ilga pieredze datu aizsardzības speciālista darbā ar datu aizsardzības prasību piemērošanu un interpretāciju?
9. Cik gadu ilga attiecīgā pieredze datu aizsardzības speciālistam ir darbā organizācijas nozarē vai jomā (vai uzdevumos, kas saistīti ar organizācijas nozari vai jomu, piemēram, konsultācijām)?
10. Cik mācību stundu katru gadu ir datu aizsardzības speciālistam, lai attīstītu un/vai saglabātu savas profesionālās īpašības un speciālās zināšanas par datu aizsardzības tiesību aktiem un praksi?
11. Vai organizācijas vadība ir skaidri definējusi un rakstiski aprakstījusi datu aizsardzības speciālista uzdevumus?
12. Vai iepriekš minētais datu aizsardzības speciālista uzdevumu rakstiskais apraksts ir darīts zināms organizācijas personālam, vai arī šie uzdevumi ir citādi paziņoti

- darbiniekiem?
13. Vai uzdevumu rakstisks apraksts atbilst un aptver visus organizācijas datu aizsardzības speciālistu faktiskos uzdevumus?
  14. Kurš no turpmāk minētajiem uzdevumiem ir uzticēts organizācijas datu aizsardzības speciālistam?
  15. Vai datu aizsardzības speciālistam ir uzticēti papildu uzdevumi salīdzinājumā ar Datu regulas paredzētajiem uzdevumiem?
  16. Vai datu aizsardzības speciālists pilda datu aizsardzības speciālista pienākumus uz pilnu slodzi?
  17. Nodrošinot pilna laika nodarbinātību, cik daudz darba laika datu aizsardzības speciālists var piešķirt datu aizsardzības speciālista uzdevumu un pienākumu veikšanai?
  18. Cik daudz pilna laika ekvivalentu ir datu aizsardzības speciālista rīcībā, pildot datu aizsardzības speciālista (piemēram, datu aizsardzības grupas, partnera(-u) vai cita līdzīga pastāvīga rakstura vienošanās) uzdevumus?
  19. Vai datu aizsardzības speciālistam ir iecelts vietnieks?
  20. Vai uzskatāt, ka iepriekš minētie resursi ir pietiekami, lai pildītu datu aizsardzības speciālista uzdevumus?
  21. Vai organizācijas datu aizsardzības speciālistam ir piešķīrusi budžetu?
  22. Ja organizācija datu aizsardzības speciālistam ir piešķīrusi budžetu, vai datu aizsardzības speciālista var pārvaldīt budžetu neatkarīgi?
  23. Ja datu aizsardzības speciālistam papildus datu aizsardzības speciālista uzdevumiem ir citi uzdevumi vai funkcijas, kādi ir šie uzdevumi vai uzdevumi?
  24. Cik iekšēju (oficiālu vai neoficiālu) konsultāciju pieprasījumu par pienākumiem saskaņā ar datu aizsardzības regulu saņem vidēji mēnesī?
  25. Cik bieži datu aizsardzības speciālists ir iesaistīts un/vai ar viņu apspriežas, risinot un risinot ar personas datu apstrādi un aizsardzību saistītus jautājumus organizācijā?
  26. Vai organizācijas iekšējos procesos ir jāapspriežas ar datu aizsardzības speciālistu par jautājumiem, kas saistīti ar datu aizsardzību, piemēram, par personas datu aizsardzības pārkāpumiem?
  27. Vai datu aizsardzības speciālistam kopumā ir piekļuve un vai viņam tiek sniegta pietiekama informācija par jautājumiem, kas saistīti ar datu aizsardzību un personas datu apstrādes darbībām organizācijā, lai veiktu savus uzdevumus?
  28. Vai kopumā organizācijā tiek ņemti vērā datu aizsardzības speciālista atzinumi?
  29. Ja organizācija neseko datu aizsardzības speciālista ieteikumam, vai ir dokumentēti

ienesli?

30. Vai organizācija dod norādījumus datu aizsardzības speciālistam par viņa uzdevumu un pienākumu izpildi?
31. Vai organizācija datu aizsardzības speciālistu ir atlaidusi no amata vai sodījusi par savu uzdevumu un pienākumu izpildi?
32. Vai ir sagaidāms, ka datu aizsardzības speciālists regulāri atskaitīsies organizācijas augstākajam vadības līmenim?
33. Kādā no turpmāk minētajiem veidiem datu aizsardzības speciālists ziņo organizācijas augstākajai un citai vadībai? Izvēlieties visas piemērojamās opcijas.
34. Vai organizācija ir publicējusi datu aizsardzības speciālista kontaktinformāciju un paziņojusi to uzraudzības organizācijai?
35. Ja organizācija ir publicējusi datu aizsardzības speciālista kontaktinformāciju, lūdzu norādiet kurā no turpmāk minētajiem līdzekļiem?
36. Vai datu subjektiem ir iespēja sazināties ar datu aizsardzības speciālistu jautājumos, kas saistīti ar viņu personas datu apstrādi vai datu subjekta tiesību īstenošanu?
37. Lūdzu, norādiet, kā datu subjekti var sazināties ar datu aizsardzības speciālistu.
38. Cik pieprasījumi no datu subjektiem tiek saņemti vidēji mēnesī?
39. Vai, jūsu prāt, datu aizsardzības uzraudzības iestādei būtu jāpublicē datu aizsardzības speciālistu kontaktinformācija (pasta adrese, īpašs tālruna numurs un/vai īpaša e-pasta adrese), lai atvieglotu pārredzamības pienākumus?
40. Kādus papildu norādījumus jūsu organizācija vēlētos saņemt no datu aizsardzības uzraudzības iestādēm, lai precizētu datu aizsardzības speciālista uzdevumus un pienākumus?

Ziņojumā sniegta informācija par koordinētās pārbaudes rezultātiem un apkopota atbilstoši organizāciju iesniegtajām atbildēm par datu aizsardzības speciālista atbilstību Datu regulas prasībām.



## 4. PĀRBAUDES REZULTĀTI

### Organizācijas loma

Atbilžu attiecība		
Pārzinis	169	94,413%
Apstrādātājs	59	32,961%

### Lūdzu norādiet nozari

Atbilžu attiecība		
Privātais sektors	5	2,793%
Publiskais sektors	174	97,207%

### Organizācija ir uzņēmuma galvenā iestāde

Atbilžu attiecība		
Jā	5	2,793%
Nē	0	
Nav atbildes	174	97,207%

### Teritoriālā kompetences joma:

Atbilžu attiecība		
Centrālā iestāde	97	54,190%
Reģionālā vai vietējā iestāde	65	36,313%
Cits:	12	6,704%
Nav atbildes	5	2,793%

### Atbildētājs ir organizācijas datu aizsardzības speciālists:

Atbilžu attiecība		
Jā	139	77,654%
Nē	34	18,994%
Nav atbildes	6	3,352%

### 1. Vai organizācija ir iecēlusi datu aizsardzības speciālistu un, ja jā, uz kāda pamata? (Datu regulas 37. panta 1. punkts un 37. panta 4. punkts)

Atbilžu attiecība		
"Jā – apstrādi veic valsts iestāde vai struktūra (izņemot tiesu, kas darbojas kā tiesnesis)."	149	83,240%
"Jā – organizācijas pamatdarbību veido apstrādes darbības, kuru rakstura, apjoma un/vai mērķu dēļ ir nepieciešama regulāra un sistemātiska datu subjektu uzraudzība plašā mērogā."	11	6,145%
"Jā – organizācijas pamatdarbība sastāv no liela mēroga īpašu kategoriju datu un/vai personas datu, kas saistīti ar sodāmību un noziedzīgiem nodarījumiem, apstrāde."	4	2,235%

"Jā – citas Savienības vai dalībvalsts tiesību aktos noteiktas prasības dēļ."	10	5,587%
Jā – uz cita pamata (piemēram, uz brīvprātības pamata).	3	1,676%
"Nē – organizācija nav iecēlusi datu aizsardzības speciālistu, jo viņa iecelšana nav obligāta."	1	0,559%
"Nē – organizācija nav iecēlusi datu aizsardzības speciālistu, lai gan viņa iecelšana būtu obligāta:"	1	0,559%

**2. Vai persona, kas iecelta par datu aizsardzības speciālistu, darbojas kā vienīgais dati aizsardzības speciālists uzņēmumu grupai vai vairākām iestādēm vai struktūrām? (Datu regulas 37. panta 2. un 37. panta 3. punkts)**

Atbilžu attiecība		
Jā:	85	47,486%
Nē	80	44,693%
Es nezinu vai nevēlos atbildēt	12	6,704%
Nav atbildes	2	1,117%

**3. Vai datu aizsardzības speciālists ir organizācijas darbinieks vai arī uzdevumi, tiek pildīti, pamatojoties uz pakalpojuma līgumu? (Datu regulas 37. panta 6. punkts)**

Atbilžu attiecība		
Darbinieks	80	44,693%
Uz pakalpojumu līgumu balstīta loma:	95	53,073%
Es nezinu vai nevēlos atbildēt	2	1,117%
Nav atbildes	2	1,117%

**4. Uz kādu termiņu datu aizsardzības speciālists ir iecelts amatā?**

Atbilžu attiecība		
Pastāvīgs/nenoteikts termiņš	90	50,279%
Uz laiku vai uz noteiktu laiku :	85	47,486%
Es nezinu vai nevēlos atbildēt	2	1,117%
Nav atbildes	2	1,117%

**5. Kurā organizācijas departamentā/nodaļā ietilpst datu aizsardzības speciālists?**

Atbilžu attiecība		
Augstākā vadība	16	8,939%
Administratīvā vadība	50	27,933%
Cilvēkresursi	2	1,117%
Informācijas pārvaldība	3	1,676%
IT vai informācijas drošības funkcija	12	6,704%
Juridiskā vai atbilstības funkcija	38	21,229%
Cita eksperta loma	27	15 084%

Jebkurš cits biroja darbinieks	2	1,117%
Cits:	26	14,525%
Es nezinu vai nevēlos atbildēt	1	0,559%
Nav atbildes	2	1,117%

**6. Kurās no tālāk norādītajām tēmām organizācijas datu aizsardzības speciālistam (vai viņa darbiniekiem) ir pieredze vai zināšanas? Izvēlieties visas piemērojamās iespējas. (Datu regulas 37. panta 5. punkts)**

Atbilžu attiecība		
Datu aizsardzības un privātuma jautājumi	170	94,972%
Informācijas drošības jautājumi	130	72,626%
Informācijas sistēmu vadība un/vai attīstība	65	36,313%
Datu aizsardzības procesi (NIDA, DS pieprasījumi, u.c.)	119	66 480%
Organizācijas nozares vai nozares biznesa procesi	97	54,190%
Tiesību akti par personas datu apstrādi un aizsardzību	159	88,827%
Uzraudzības iestāžu pamatnostādnes par personas datu apstrādi	115	64,246%
Īpaši tiesību akti, kas attiecas uz organizācijas nozari vai jomu	117	65,363%
Es nezinu vai nevēlos atbildēt	1	0,559%
Nav atbildes	2	1,117%

**7. Kuri no turpmāk minētajiem faktoriem, ieceļot datu aizsardzības speciālistu, tika noteikti kā prasības amatam?**

Atbilžu attiecība		
Ekspertu zināšanas par datu aizsardzības regulējumu	157	87,709%
Ekspertu zināšanas par datu aizsardzības praksi	129	72,067%
Ekspertu zināšanas par datu aizsardzības prasībām, kas izriet no īpašiem tiesību aktiem, kas attiecas uz organizācijas nozari vai jomu	100	55,866%
Spēja izpildīt uzdevumus saskaņā ar Datu regulu	157	87,709%
Citas profesionālās kvalifikācijas	99	55,307%
Nav īpašu zināšanu datu aizsardzības jomā, bet norādīšana bija obligāta	3	1 676%
Cits:	6	3352%
Nav atbildes	2	1,117%

**8. Cik gadu pieredze datu aizsardzības speciālistam ir datu aizsardzības prasību piemērošanā un interpretācijā? (Datu regulas 37. panta 5. punkts)**

Atbilžu attiecība		
<1 gads	5	2,793%
1–2 gadi	15	8,380%
3–5 gadi	55	30,726%

6–8 gadi	33	18,436%
>8 gadi	62	34,637%
Es nezinu vai nevēlos atbildēt	7	3,911%
Nav atbildes	2	1,117%

**9. Cik gadu attiecīgā pieredze datu aizsardzības speciālistam ir darbā organizācijas nozarē vai jomā (vai uzdevumos, kas saistīti ar organizācijas nozari vai jomu, piemēram, konsultācijām)?**

Atbilžu attiecība		
<1 gads	3	1,676%
1–2 gadi	15	8,380%
3–5 gadi	51	28,492%
6–8 gadi	29	16,201%
>8 gadi	72	40,223%
Es nezinu vai nevēlos atbildēt	7	3,911%
Nav atbildes	2	1,117%

**10. Cik mācību stundu katru gadu ir datu aizsardzības speciālistam, lai attīstītu un/vai saglabātu savas profesionālās īpašības un speciālās zināšanas par datu aizsardzības tiesību aktiem un praksi?**

Atbilžu attiecība		
0 stundas gadā	5	2,793%
1–8 stundas gadā	18	10,056%
9–16 stundas gadā	50	27,933%
17–24 stundas gadā	13	7,263%
25–32 stundas gadā	13	7,263%
> 32 stundas gadā	58	32,402%
Es nezinu vai nevēlos atbildēt	20	11,173%
Nav atbildes	2	1,117%

**11. Vai organizācijas vadība ir skaidri definējusi un rakstiski aprakstījusi datu aizsardzības speciālista uzdevumus?**

Atbilžu attiecība		
Jā	169	94,413%
Nē	5	2,793 %
Es nezinu vai nevēlos atbildēt	3	1,676%
Nav atbildes	2	1,117%

**12. Vai iepriekš minētais datu aizsardzības speciālista uzdevumu rakstiskais apraksts ir darīts zināms organizācijas personālam, vai arī šie uzdevumi ir citādi paziņoti darbiniekiem?**

Atbilžu attiecība		
-------------------	--	--

Jā	159	88,827%
Nē	10	5,587%
Es nezinu vai nevēlos atbildēt	8	4,469%
Nav atbildes	2	1,117%

**13. Vai uzdevumu rakstisks apraksts atbilst un aptver visus organizācijas datu aizsardzības speciālistu faktiskos uzdevumus?**

Atbilžu attiecība		
Jā	160	89,385%
Nē	10	5,587%
Es nezinu vai nevēlos atbildēt	7	3,911%
Nav atbildes	2	1,117%

**14. Kurš no turpmāk minētajiem uzdevumiem ir uzticēts organizācijas datu aizsardzības speciālistam? Izvēlieties visas piemērojamās opcijas. (Datu regulas 39. panta 1. punkts, 38. panta 3. punkts, 38. panta 4. punkts un 38. panta 6. punkts)"**

Atbilžu attiecība		
Informēšana un konsultēšana par pienākumiem saskaņā ar datu aizsardzības regulu	173	96,648%
Organizācijas politiku izstrāde un uzturēšana saistībā ar personas datu aizsardzību	158	88,268%
Piedalīšanās jaunu procedūru vai esošo procedūru izmaiņu plānošanā, kas ietver personas datu apstrādi	158	88,268%
Personas datu apstrādes un aizsardzības uzraudzība	171	95,531%
Organizācijas personāla apmācība saistībā ar datu aizsardzību	163	91,061%
Konsultāciju sniegšana par datu aizsardzības ietekmes novērtējumiem	157	87,709 %
Datu aizsardzības ietekmes novērtējumu izpildes uzraudzība	138	77,095%
Piedalīšanās personas datu aizsardzības pārkāpumu apstrādē	167	93,296%
Ziņošana organizācijas vadībai par organizācijas statusu un attīstības vajadzībām datu aizsardzības jomā	153	85,475%
Uzraudzīt svarīgākās izmaiņas un aktuālos jautājumus, kas ietekmē datu aizsardzību organizācijas nozarē vai jomā un ziņot par tiem organizācijas vadībai	137	76,536%
Darbojoties kā datu aizsardzības uzraudzības organizācijas kontaktpunkts	153	85,475%
Darbojoties kā datu subjektu kontaktpunktam, jo īpaši tad, kad tie izmanto savas tiesības	147	82,123%
Es nezinu vai nevēlos atbildēt	3	1,676%
Nav atbildes	2	1,117%

**15. Vai datu aizsardzības speciālistam ir uzticēti papildu uzdevumi salīdzinājumā ar Datu regulas paredzētajiem uzdevumiem?**

Atbilžu attiecība		
Lēmumu pieņemšana par personas datu apstrādi	37	20,670%
Organizācijas datu aizsardzības procesu attīstīšana	105	58,659%
datu aizsardzības ietekmes novērtējumu izstrāde un/vai veikšana	73	40,782 %
Datu subjektu pieprasījumu izpilde par viņu datu aizsardzības tiesībām	106	59,218%
Līgumu (piem., datu apstrādes līgumu) izstrāde un/vai sarunu vešana	109	60,894%
Atbildība par personas datu apstrādes likumību	48	26,816%
Cīts:	15	8,380%
Es nezinu vai nevēlos atbildēt	14	7,821%
Nav atbildes	2	1,117%

**16. Vai datu aizsardzības speciālists pilda datu aizsardzības speciālista pienākumus uz pilnu slodzi?**

Atbilžu attiecība		
Jā, datu aizsardzības speciālista uzdevumi ir personas galvenais amata apraksts	93	51 955%
Nē, datu aizsardzības speciālista uzdevumi tiek veikti papildus citiem uzdevumiem, bet ne kā pamatuzdevumi	67	37 430%
Es nezinu vai nevēlos atbildēt	17	9,497%
Nav atbildes	2	1,117%

**17. Nodrošinot pilna laika nodarbinātību, cik daudz darba laika datu aizsardzības speciālists var piešķirt datu aizsardzības speciālista uzdevumu un pienākumu veikšanai**

Atbilžu attiecība		
91–100 %	33	18,436 %
71–90%	3	1,676%
51–70%	5	2,793%
31–50 %	14	7,821%
21–30 %	14	7,821%
11–20 %	24	13,408 %
6–10%	13	7,263%
Mazāk nekā 5 %	5	2,793%
Persona, kas iecelta par datu aizsardzības speciālistu, ir nepilna laika	50	27,933%
Es nezinu vai nevēlos atbildēt	16	8,939%
Nav atbildes	2	1,117%

**18. Cik daudz pilna laika ekvivalentu ir datu aizsardzības speciālista rīcībā, pildot datu aizsardzības speciālista (piemēram, datu aizsardzības grupas, partnera(-u) vai cita līdzīga pastāvīga rakstura vienošanās) uzdevumus? (Datu regulas 38. panta 2. punkts)**

Atbilžu attiecība		
Nav (0 FTE)	24	13,408%
0–0,9 FTE (nepilna laika resurss)	62	34,637%
1,0–2,0 FTE	11	6,145%
2,1–4,0 FTE	14	7,821%
>6 FTE	2	1,117%
Es nezinu vai nevēlos atbildēt	64	35,754%
Nav atbildes	2	1,117%

**19. Vai datu aizsardzības speciālistam ir iecelts vietnieks?**

Atbilžu attiecība		
Jā	51	28,492%
Nē	123	68,715%
Es nezinu vai nevēlos atbildēt	3	1,676%
Nav atbildes	2	1,117%

**20. Vai uzskatāt, ka iepriekš minētie resursi ir pietiekami, lai pildītu datu aizsardzības speciālista uzdevumus (Datu regulas 38. panta 2. punkts)**

Atbilžu attiecība		
Jā	147	82,123%
Nr	19	10,615%
Es nezinu vai nevēlos atbildēt	11	6,145%
Nav atbildes	2	1,117%

**21. Vai organizācija datu aizsardzības speciālistam ir piešķirusi budžetu?**

Atbilžu attiecība		
jā	63	35,196%
Nē	100	55,866%
Es nezinu vai nevēlos atbildēt	14	7,821%
Nav atbildes	2	1,117%

**22. Ja organizācija datu aizsardzības speciālistam ir piešķirusi budžetu, vai datu aizsardzības speciālists var pārvaldīt budžetu neatkarīgi?**

Atbilžu attiecība		
Jā	26	14,525%
Nē:	29	16,201%
Es nezinu vai nevēlos atbildēt	8	4,469%

Nav atbildes	116	64,804%
--------------	-----	---------

**23. Ja datu aizsardzības speciālistam papildus datu aizsardzības speciālista uzdevumiem ir citi uzdevumi vai funkcijas, kādi ir šie uzdevumi? Ja ir vairākas, izvēlieties visas atbilstošās opcijas. (Datu regulas 38. panta 2. un 38. panta 6. punkts)"**

Atbilžu attiecība		
Pārvaldība:	22	12,291%
IT vai informācijas drošība:	31	17,318%
Likums vai atbilstība:	31	17,318%
Cita eksperta loma:	19	10,615%
Cits:	34	18,994%
Es nezinu vai nevēlos atbildēt	99	55,307%
Nav atbildes	2	1,117%

**24. Cik iekšēju (oficiālu vai neoficiālu) konsultāciju pieprasījumu par pienākumiem saskaņā ar datu aizsardzības regulu saņem vidēji mēnesī? (Datu regulas 39. panta 1. punkts)**

Atbilžu attiecība		
0–10	126	70,391%
11–20	36	20,112%
21–30	6	3,352%
31–40	2	1,117%
>40	6	3,352%
Es nezinu vai nevēlos atbildēt	1	0,559%
Nav atbildes	2	1,117%

**25. Cik bieži datu aizsardzības speciālists tiek iesaistīts un/vai ar to apspriežas un risinot jautājumus, kas saistīti ar personas datu apstrādi un aizsardzību iestādē? (Datu regulas 38. panta 1. punkts)"**

Atbilžu attiecība		
Visu laiku (100 %)	48	26,816%
75–99 % laika	42	23,464 %
50–74 % laika	12	6,704 %
25–49 % laika	24	13,408 %
5–24 % laika	32	17,877 %
Mazāk nekā 5 % laika	10	5,587 %
Es nezinu un nevēlos atbildēt	9	5,028%
Nav atbildes	2	1,117%

**26. Vai organizācijas iekšējos procesos ir jāapspriežas ar datu aizsardzības speciālistu par jautājumiem, kas saistīti ar datu aizsardzību, piemēram, par personas datu aizsardzības pārkāpumiem?**



Atbilžu attiecība		
Jā, visos ar personas datu apstrādi saistītajos procesos	141	78,771%
Jā, dažos ar personas datu apstrādi saistītajos procesos	29	16,201%
Nē	4	2,235%
Es nezinu vai nevēlos atbildēt	3	1,676%
Nav atbildes	2	1,117%

**27. Vai datu aizsardzības speciālistam kopumā ir piekļuve un vai viņam tiek sniegta pietiekama informācija par jautājumiem, kas saistīti ar datu aizsardzību un personas datu apstrādes darbībām organizācijā, lai veiktu savus uzdevumus? (Datu regulas 38. panta 1. punkts un 38. panta 2. punkts)**

Atbilžu attiecība		
Visu laiku	98	54,749%
Lielāko daļu laika	73	40,782%
Dažreiz	5	2,793%
Es nezinu vai nevēlos atbildēt	10	5,59%
Nav atbildes	2	1,117%

**28. Vai kopumā datu aizsardzības speciālista atzinumi tiek ievēroti? (Datu regulas 38. panta 1. punkts un 39. pants)**

Atbilžu attiecība		
Ļoti labi	92	51,397%
Labi	77	43,017%
vidējais	7	3,911%
Es nezinu vai nevēlos atbildēt	1	0,559%
Nav atbildes	2	1,117%

**29. Ja organizācija neievēro datu aizsardzības speciālista ieteikumu, vai iemesli ir dokumentēti? (Datu regulas 38. panta 1. punkts)**

Atbilžu attiecība		
Visu laiku	48	26,816%
Lielāko daļu laika	42	23,464%
Dažreiz	9	5,028%
Reti	5	2,793%
Nekad	33	18,436%
Es nezinu vai nevēlos atbildēt	40	22,346%
Nav atbildes	2	1,117%

**30. Vai organizācija sniedz norādījumus datu aizsardzības speciālistam par viņa uzdevumu un pienākumu izpildi? (Datu regulas 38. panta 3. punkts un 38. panta 6. punkts)**

Atbilžu attiecība		
-------------------	--	--

Jā	59	32,961%
Nē	106	59,218%
Es nezinu vai nevēlos atbildēt	12	6,704%
Nav atbildes	2	1,117%

**31. Vai organizācija kādreiz ir atlaidusi vai sodījusi datu aizsardzības speciālistu par viņa uzdevumu un pienākumu veikšanu? (Datu regulas 38. panta 3. punkts)**

Atbilžu attiecība		
Nē	177	98,883%
Nav atbildes	2	1,117%

**32. Vai ir sagaidāms, ka datu aizsardzības speciālists regulāri atskaitīsies organizācijas augstākajam vadības līmenim?**

Atbilžu attiecība		
0 reizes gadā, atskaites nav paredzētas	26	14,525%
0 reizes gadā, lai gan ziņošana ir paredzēta	8	4,469%
1–2 reizes gadā	89	49,721%
3–4 reizes gadā	9	5,028%
>4 reizes gadā	37	20,670%
Es nezinu vai nevēlos atbildēt	8	4,469%
Nav atbildes	2	1,117%

**33. Kādā no turpmāk minētajiem veidiem datu aizsardzības speciālists ziņo organizācijas augstākajai un citai vadībai? Izvēlieties visas piemērojamās opcijas.**

Atbilžu attiecība		
Nav	14	7,821%
Valdei iesniegts un/vai iesniegts rakstisks ziņojums	79	44,134%
Vadības grupai(-ām) iesniegts un/vai iesniegts rakstisks ziņojums	45	25,140%
Cits:	43	24,022%
Es nezinu vai nevēlos atbildēt uz	9	5,028%
Nav atbildes	2	1,117%

**34. Vai organizācija ir publicējusi datu aizsardzības speciālista kontaktinformāciju un paziņojusi to uzraudzības iestādei? (Datu regulas 37. panta 7. punkts)**

Atbilžu attiecība		
Jā, abi	172	96,089%
Ir publicēts, bet nav paziņots	3	1,676%
Es nezinu vai nevēlos atbildēt	2	1,117%
Nav atbildes	2	1,117%

**35. Ja organizācija ir publicējusi datu aizsardzības speciālista kontaktinformāciju, lūdzu norādīt, kurā no turpmāk minētajiem līdzekļiem? (Datu regulas 37. panta 7. punkts)**

Atbilžu attiecība		
Privātuma/citas informācijas paziņojums	111	62,011%
Organizācijas publiskā tīmekļa vietne	167	93,296%
Cits(-i) publiskais(-i) kanāls(-i)	8	4,469%
Organizācijas iekšējais iekštīkls	84	46,927%
Cits(-i) iekšējais(-i) kanāls(-i)	21	11,732%
Nav atbildes	2	1,117%

**36. Vai datu subjektiem ir iespēja sazināties ar datu aizsardzības speciālistu jautājumos, kas saistīti ar viņu personas datu apstrādi vai datu subjekta tiesību īstenošanu? (Datu regulas 38. panta 4. punkts)**

Atbilžu attiecība		
Jā:	176	98,324%
Es nezinu vai nevēlos atbildēt	10	5,59%
Nav atbildes	2	1,117%

**37. Lūdzu, norādiet kā datu subjekti var sazināties ar datu aizsardzības speciālistu (visas piemērojamās iespējas)**

Atbilžu attiecība		
E-pasts	174	97,207%
Tīmekļa ziņojums (vai cits līdzvērtīgs) tiešsaistes pakalpojumā	10	5,587%
Tālrunis	124	69,274%
Pasts	76	42,458%
Cits:	3	1,676%
Nav atbildes	3	1,676%

**38. Cik pieprasījumi no datu subjektiem tiek saņemti vidēji mēnesī (Datu regulas 38. panta 4. punkts)**

Atbilžu attiecība		
0–10	167	93,296%
11–20	2	1,117%
21–30	1	0,559%
Es nezinu vai nevēlos atbildēt	7	3,911%
Nav atbildes	2	1,117%

**39. Vai, jūsu prāt, datu aizsardzības uzraudzības iestādei būtu jāpublicē datu aizsardzības speciālistu kontaktinformācija (pasta adrese, īpašs tālruna numurs un/vai īpaša e-pasta adrese), lai atvieglotu pārredzamības pienākumus ?**

Atbilžu attiecība		
-------------------	--	--

Jā	114	63,687%
Nē	44	24,581%
Es nezinu vai nevēlos atbildēt	21	11,732%

**40. Kādus turpmākus norādījumus jūsu organizācija vēlētos saņemt no datu aizsardzības uzraudzības iestādēm, lai precizētu datu aizsardzības speciālista uzdevumus un lomu? Izvēlieties visas piemērojamās iespējas.**

Atbilžu attiecība		
Jautājumi un atbildes / BUJ	125	69,832%
Tiešsaistes rīki	89	49,721%
Papildu vadlīnijas	127	70,950%
Mācību materiāli vai dokumenti datu aizsardzības speciālistiem	137	76,536%
Apmācību materiāli vai dokumenti, ko izplatīt organizācijas iekšienē	128	71,508%
Cits:	2	1,117%
Papildu norādījumi netiek uzskatīti par nepieciešamiem	9	5,028%

## 5. ATBILŽU KOPSAVILKUMS

1. Kopumā pārbaudes ietvaros tika saņemtas 179 aizpildītas aptaujas anketas no ministrijām, to padotības iestādēm, kā arī no asociācijām. 169 iestādēm vai 94.41 % no tiem, kas piedalījušies aptaujā norādījuši, ka organizācijas sevi identificē kā ir pārzinis. 59 organizācijas vai 32.96 % no visiem aptaujātajiem sevi identificē ar apstrādātāja lomu. Daļa no aptaujātajiem norādījuši abas lomas, kas liek domāt ka organizācijām lomas var mainīties atkarībā no konkrētās apstrādes un no izrietošajiem pienākumiem.

Absolūtais vairākums no aptaujātajiem, vai 174 no aptaujātajiem sevi identificē kā publiskā sektora organizācijas.

2. 77.65 % Aptaujas anketas sagatavojis organizācijas datu aizsardzības speciālists. Un tikai 18.99 % no aizpildītajām aptaujas anketām gatavoja persona, kas nav organizācijas datu aizsardzības speciālists. 3.35 % no aizpildītajām aptaujas anketām nevēlējās atbildēt uz šo jautājumu.

3. Gandrīz visām (99%) organizāciju ir iecelts datu aizsardzības speciālists.

4. 83 % organizācijas to ir iecēlušas pamatojoties uz Datu regulas 37.panta 1. punkta a) apakšpunktu (apstrādi veic publiska iestāde vai struktūra). 6 % aptaujāto pamatojās uz Datu regulas 37.panta 1.punkta b) apakšpunktu (pārziņa vai

apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām to būtības, apmēra un/vai nolūku dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā).

5. No minētā secināms, ka organizācijas ir iecēlušas datu aizsardzības speciālistu un tie ieņem nozīmīgu lomu personas datu apstrādes atbilstības veicināšanā organizācijā. Daudzos gadījumos prasība iecelt datu aizsardzības speciālistu ir pamatota ar Datu regulā noteiktajiem pienākumiem, savukārt dažos gadījumos ir konstatēts, ka to nosaka citi normatīvie akti. Tas liecina, ka likumdevējs, ieviešot šos papildu regulējošos pasākumus, ir ņēmis vērā ar datu aizsardzību saistītos riskus, kā arī pieaugošo digitalizācijas procesu attīstību un no tās izrietošos nākotnes izaicinājumus personas datu apstrādes jomā. Tā kā digitalizācijas apmēri turpina paplašināties praktiski visās nozarēs, un to pavada no digitalizācijas izrietošie riski datu aizsardzībā, ir nepieciešamas arvien augstākas prasības pēc datu drošības, un ir saprotama pārziņu vēlme noteikt augstākas prasības attiecībā uz datu aizsardzību un noteikt pienākumu iecelt datu aizsardzības speciālistu, kas tieši būtu atbildīgas par personas datu apstrādes procesu atbilstības vērtēšanu organizācijā.
6. Attiecība starp organizācijām, kas piesaista ārpalpojumu sniedzējus datu aizsardzības speciālista pakalpojumu sniegšanai, ir līdzīgas pret tām organizācijām, kuras ieceļ speciālistus no saviem iekšējiem resursiem. Tas nozīmē, ka organizācijas pieņem dažādus pasākumus, lai izpildītu savus datu aizsardzības pienākumus, un to izvēle pamatosies uz resursu (cilvēkresursi, finansiālie, tehniskie utt.) pieejamības faktoriem. Ņemot vērā aptaujāto iestāžu atšķirīgo lielumu un no tām izrietošās vajadzības, ir saprotams, ka visām organizācijām neder viens vienots modelis attiecībā uz datu aizsardzības speciālista norīkošanu. Šāda tendence ar līdzīgu attiecību ir iezīmējusies arī iepriekšējos gados veiktajās aptaujās par datu aizsardzības speciālista iecelšanu.
7. Neskatoties uz to, ka tā ir salīdzinoši jauna profesija, vairāk nekā 50% no aptaujātajiem ir 6 vai vairāk gadu pieredze datu aizsardzībā un gandrīz 35% ir vairāk nekā 8 gadu pieredze šajā jomā. No minētā secināms, ka personas datu aizsardzība nesākās tikai Datu regulas piemērošanas datumu, bet organizatorisko un tehnisko pasākumu ieviešana datu aizsardzības veicināšanai ir notikusi arī agrāk.
8. Kopumā datu aizsardzības speciālistu padomi un ieteikumi organizācijas turpmākās darbības gaitā tiek ņemti vērā 94% gadījumu, kas liecina par uzticēšanos un sava veida datu aizsardzības speciālista viedokļa respektēšanu iestādēs.

9. Gandrīz 28% no anketām norādīts, ka datu aizsardzības speciālista amats ietilpst administratīvās vadības sadaļā, 9% tas ietilpst augstākās vadības sadaļā, 21% no organizācijām datu aizsardzības speciālista amats ietilpst juridiskajā vai atbilstības funkciju nodrošinošajā nodaļā, savukārt, 6,7% tas ietilpst IT vai informācijas drošības funkciju nodrošinošajā nodaļā un 35 % ir norādījuši citu nodaļu, kur ietilpst datu aizsardzības speciālists.
10. Nedaudz vairāk kā pusei (52%) aptaujāto datu aizsardzības speciālists ir pilna laika darbinieks. Šī attiecība ir diezgan līdzīga ar ārštata un no saviem resursiem iecelto datu aizsardzības speciālistu attiecību kas savukārt liecina, ka vairumā gadījumu no saviem resursiem ieceltais datu aizsardzības speciālists, pilda savus pienākumus, savienojot to ar citu amatu. Kas savukārt liecina, ka organizācija ir iecēlusi to no saviem resursiem, ņemot vērā tā kvalifikācijas un speciālo zināšanu līmeni un/vai veikusi kvalifikācijas paaugstināšanu konkrētajam darbiniekam lai viņš varētu pildīt arī datu aizsardzības speciālista pienākumus.
11. Vairumā gadījumu, jeb 93% iestāžu saņem līdz 10 datu subjektu pieprasījumiem mēnesī un tikai dažos gadījumos (3) šis skaitlis bija lielāks.

## 6. SECINĀJUMI

- Kopumā atbildes uz šo aptaujas anketu un no tās izrietošās tendences ir līdzīgas ar iepriekšējos gados veiktajām aptaujām. Piemēram, attiecība ar iecelto datu aizsardzības speciālistu no saviem resursiem ar attiecību, kur datu aizsardzības speciālists ir ārpalpojums ir līdzīga ar iepriekšējā gadā veiktās aptaujas rezultātiem, kas liecina par zināmu praksi
- Lai gan kopējie aptaujas rezultāti liecina, ka organizācijas kopumā saprot un novērtē datu aizsardzības speciālista lomu, ir skaidrs, ka šajā ziņā ir iespējami uzlabojumi. Piemēram, bažas rada tas, ka tikai 30% respondentu ir iecēluši datu aizsardzības speciālista aizstājēju, kas var būt ļoti svarīgi, ja speciālists ir atvaļinājumā vai nav pieejams personisku iemeslu dēļ.
- Inspekcijai bažas raisa fakts ka gandrīz 28% no organizācijām datu aizsardzības speciālista amats ietilpst juridiskajā, atbilstības funkciju nodrošinošajā vai IT, vai informācijas drošības funkciju nodrošinošajā nodaļā, kas pirmšķietami liecina par interešu konflikta

risku. Lai konstatētu vai atspēkotu iepriekš minēto secinājumu, šim aspektam būtu nepieciešama padziļinātāka analīze.

- Vēl viens satraucošs aspekts ir tas, ka vairāk nekā 30% iestāžu sniedz norādījumus datu aizsardzības speciālistam par viņu uzdevumiem un pienākumiem. Tas rada bažas par speciālista neatkarību, saņemot norādījumus no vadības. Arī šis, iespējams, būtu padziļināti pētāms jautājums, proti, vai norādījumu sniegšana datu aizsardzības speciālistam par viņu uzdevumiem un pienākumiem nenonāk pretstatā ar Datu regulas 38. pantā noteikto, ka datu aizsardzības speciālists nedrīkst saņemt nekādus norādījumus attiecībā uz tam minēto uzdevumu veikšanu.
- Vairumā gadījumu organizācijas ir ieinteresētas un vēlas lai datu aizsardzības uzraudzības iestāde publicē papildus materiālus, kas precizētu datu aizsardzības speciālista uzdevumus un lomu.
- Kopumā aptauja atklāj pozitīvas tendences attiecībā uz datu aizsardzības speciālista lomu organizācijās. Tomēr dažās jomās pastāv pretrunas, iespējams, tāpēc, ka trūkst pilnīgas izpratnes par datu aizsardzības speciālista lomu. Tas uzsver nepieciešamību turpināt centienus stiprināt datu aizsardzības speciālista lomu, kā arī lai veicināt tā atpazīstamību un uzsvērt tā nozīmi datu aizsardzības kontekstā.

## **7. IETEIKUMI**

- Stiprināt datu aizsardzības speciālista institūtu, turpinot organizāciju izglītošanu par tā nepieciešamību, statusu, kompetencēm.
- Veikt izpēti par norādījumu sniegšanu datu aizsardzības speciālistam par viņu uzdevumiem un pienākumiem un vai tas nenonāk pretstatā ar Datu regulas 38. pantā noteikto, ka datu aizsardzības speciālists nedrīkst saņemt nekādus norādījumus attiecībā uz tam minēto uzdevumu veikšanu.
- Veikt izpēti, kādos gadījumos datu aizsardzības speciālista amats ietilpstot juridiskajā, atbilstības funkciju nodrošinošajā vai IT, vai informācijas drošības funkciju nodrošinošajā nodaļā radīs interešu konfliktu.
- Izstrādāt skaidrojumus par datu aizsardzības speciālista potenciālā interešu konflikta iespējamiem gadījumiem, to novēršanu un turpmāku nepieļaušanu.