Aktualizēts: 06.05.2026.

# Centrālās statistikas pārvaldes
# prasības ārpakalpojuma sniedzējiem

Centrālajai statistikas pārvaldei (Reģ. Nr.: LV90000069830), turpmāk tekstā – Pasūtītājs ir svarīgi nodrošināt nepārtrauktu informācijas (tai skaitā, personas datu) konfidencialitāti, integritāti, pieejamību un noturību.

**Dokumentā lietotie termini un definīcijas:**

*Informācijas un komunikācijas tehnoloģiju resursi* (turpmāk – IKT resursi) - tehnisko resursu un informācijas resursu kopums, piemēram: serveri, datortīkli, ugunsmūri, datu glabāšanas iekārtas, darba stacijas, tīkla aktīvie elementi un citi IKT infrastruktūras elementi.

*Informācijas resurss* - strukturēts digitālo datu kopums, kas tiek elektroniski apstrādāts informācijas sistēmā, piemēram: datubāzes, dokumentu krājumi, reģistru ieraksti.

*Tehniskais resurss* - aparatūra, iekārta, kas ir tīkla vai informācijas sistēmas sastāvdaļa, vai IKT infrastruktūrā izmantota iekārta, kas veic datu apmaiņu ar informācijas sistēmu, un programmatūra, tostarp operētājsistēmas, sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas.

*Konfidenciāla informācija* - Prasību izpratnē ir jebkāda Pasūtītāja pārziņā esoša informācija, tajā skaitā personas dati, kurai ārpakalpojuma sniedzējs (turpmāk – Piegādātājs) piekļūst, vai var piekļūt (tai skaitā, bet ne tikai tehniskā informācija, informācija par tehnoloģijām, sistēmu piekļuves dati, tehniskie resursi, informācijas resursi un to rezerves kopijas, personas dati) jebkādā formā, tai skaitā informācijas sistēmās un papīra dokumentu formā, izņemot publiski pieejamu informāciju.

Šīs prasības (turpmāk – Prasības) ir saistošas ikvienam Piegādātājam, kurš veic Pasūtītāja pārziņā esošas Konfidenciālas informācijas apstrādi (piemēram, informācijas sistēmas uzturēšana vai izstrāde) vai pastāv varbūtība, ka var piekļūt tiešā vai netiešā veidā Konfidenciālai informācijai, tai skaitā Konfidenciālu informāciju saturošām lietām (piemēram, informācijas sistēmām, ierīcēm, iekārtām, mēbelēm, mantām), izpildot Pasūtītāja uzdevumu vai citādi sadarbojoties ar Pasūtītāju (turpmāk – Pakalpojums), piemēram, bet ne tikai, sniedzot vai saņemot pakalpojumu, sniedzot IKT resursu piegādi, sniedzot ārpakalpojumu IKT resursam, veicot būvdarbus, piegādājot preces, sadarbojoties līguma ietvaros, u.t.t.

Pasūtītājs ir noteicis Prasības, lai nodrošinātu, ka Piegādātājs atbilst, starptautisko standartu rekomendācijās, Eiropas Parlamenta un Padomes regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk - VDAR), Starptautisko un Latvijas Republikas nacionālo sankciju likuma, Nacionālā kiberdrošības likuma, Ministru kabineta 2025. gada 2. jūlija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" un citos normatīvajos aktos noteiktajām prasībām.

Prasības attiecināmas, ciktāl tās ir piemērojamas, nepārkāpjot tiesību aktos noteikto nozares speciālo regulējumu.

## 1. Vispārīgie noteikumi

1.1. Piegādātājs – privātpersona, apliecina, ka:

1.1.1. ir juridiska persona, kas ir reģistrēta NATO, Eiropas Savienības, Eiropas Brīvās tirdzniecības asociācijas (turpmāk – EBTA) vai NATO Indijas un Klusā okeāna reģiona sadarbības valstī (turpmāk – IP4 valsts) dalībvalstī vai ir fiziska persona, kas ir Latvijas Republikas valsts piederīgais, NATO, Eiropas Savienības, EBTA vai IP4 valsts pilsonis;

1.1.2. Piegādātāja juridiskās personas valde un padome sastāv no fiziskām personām, kuras nav Krievijas Federācijas, Baltkrievijas Republikas vai valsts, kuru Eiropas Parlaments vai Latvijas Republikas Saeima ir atzinusi par terorismu atbalstošu valsti valsts pilsoņi;

1.1.3. pret to nav piemērotas starptautiskās vai nacionālās sankcijas vai būtiskas finanšu un kapitāla tirgus intereses ietekmējošas Eiropas Savienības vai Ziemeļatlantijas līguma organizācijas dalībvalsts noteiktās sankcijas. Piegādātājam ir pienākums divu dienu laikā paziņot Pasūtītājam par jebkuriem apstākļiem, kas var būt par pamatu šā punkta piemērošanai.

## 2. Tiesības un pienākumi

### 2.1. Pasūtītājam ir tiesības:

2.1.1. pastāvīgi uzraudzīt pakalpojuma sniegšanas vai saņemšanas kvalitāti. Pasūtītāja atbildīgā persona par pakalpojuma uzraudzību ir noteikta savstarpēji noslēgtajā tiesiskajā darījumā (piemēram, Līgumā) vai Pasūtītāja paziņojumā Piegādātājam;

2.1.2. saņemt Pakalpojuma uzraudzībai nepieciešamo informāciju, tai skaitā žurnālfailus;

2.1.3. dot Piegādātājam vai saņēmējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar pakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;

2.1.4. iesniegt Piegādātājam vai saņēmējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt noslēgto tiesisko darījumu (piemēram, Līgumu), ja Pasūtītājs konstatējis, ka Piegādātājs nepilda tiesiskajā darījumā noteiktās prasības attiecībā uz pakalpojuma apjomu vai kvalitāti;

2.1.5. Satversmes aizsardzības birojs saskaņā ar 2021. gada 6. jūlija Ministru kabineta noteikumu Nr. 508 “Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība” 16.punktu var pārbaudīt Piegādātāju nodarbinātos, valdes locekļus un īpašniekus, kuriem Pakalpojuma izpildes laikā ir pieeja Pasūtītāja infrastruktūras funkcionēšanai nozīmīgai informācijai vai tehnoloģiskajām iekārtām vai kuri sniedz infrastruktūras funkcionēšanai nozīmīgus pakalpojumus.

2.1.6. reizi kalendārajā mēnesī vienpusēji veikt izmaiņas šajās Prasībās.

### 2.2. Piegādātāja pienākumi:

2.2.1. nodrošināt Pasūtītājam iespēju pastāvīgi uzraudzīt Pakalpojuma sniegšanas vai saņemšanas kvalitāti;

2.2.2. ievērot uz Piegādātāja un Pasūtītāja sadarbību pēc tās rakstura un būtības attiecināmos Latvijas Republikā piemērojamos normatīvos aktus, savstarpēji noslēgtā tiesiskā darījuma noteikumus, šīs Prasības, un nodrošināt Piegādātāja un tā darbības atbilstību iepriekš minētajam;

2.2.3. nodrošināt Konfidenciālas informācijas aizsardzību šajās Prasībās noteiktajā kārtībā. Gadījumā, ja starp Piegādātāju un Pasūtītāju noslēgtajā tiesiskajā darījumā ir ietverta informācijas klasifikācija, Piegādātājam ir pienākums nodrošināt tiesiskajā darījumā (piemēram, Līgumā) noteikto informācijas klasifikāciju un aizsardzību papildus šīm Prasībām. Piegādātājs nekavējoties informē Pasūtītāju gadījumā, ja Piegādātājs neatbilst Prasībām, vai nevar izpildīt kādu no Prasībās ietvertajiem norādījumiem;

2.2.4. jebkādu izmaiņu gadījumā, kas ietekmē vai var ietekmēt Piegādātāja un tā darbības atbilstību šīm Prasībām, Piegādātājs nekavējoties informē Pasūtītāju pirms minēto izmaiņu ieviešanas, kā arī pēc Pasūtītāja pieprasījuma pārskata savas darbības atbilstību šīm Prasībām un sniedz Pasūtītājam rakstisku novērtējumu par Piegādātāja un tā darbības atbilstību šīm Prasībām vai par neatbilstīgajiem aspektiem;

2.2.5. informēt par apakšuzņēmēju un viņa atbilstību šajos noteikumos un savstarpēji noslēgtajā tiesiskajā darījumā noteiktajām drošības prasībām;

2.2.6. nodrošināt, ka uz apakšuzņēmēju attiecināmi visi savstarpēji noslēgto tiesisko darījumu (piemēram, Līgumu) un šo Prasību noteikumi;

2.2.7. savstarpēji noslēgtā tiesiskā darījuma darbības laikā nekavējoties ziņot par patiesā labuma guvēja maiņu;

2.2.8. nodrošināt visu Pakalpojuma izpildei izmantoto Pasūtītāja datu (piemēram, Pasūtītāja dati, kas atrodas Piegādātāja uzturētā informācijas sistēmā) drošu nodošanu vai dzēšanu Pasūtītājam līguma izbeigšanas gadījumā vai pēc Pasūtītāja pieprasījuma;

2.2.9. iepazīties ar Pasūtītāja privātuma politiku, kas pieejama tīmekļa vietnē: https://www.csp.gov.lv/lv/privatuma-politika;

2.2.10. Piegādātājam un tā apakšuzņēmējam ir pienākums pirms katra kalendārā mēneša ietvaros sniedzamā vai saņemamā pakalpojuma vai piegādes, iepazīties ar aktuālo šī dokumenta redakciju. Aktuālā redakcija pieejama Pasūtītāja tīmekļvietnē https://www.csp.gov.lv/lv/informacijas-drosibas-pamatnostadnes.

**2.3. Piegādātāja pienākumi informācijas drošības incidentu un apdraudējumu gadījumos:**

2.3.1. tiklīdz tam kļuvis zināms ar Pasūtītāja informāciju saistīts drošības incidents un/vai Konfidenciālas informācijas, t.sk. Pasūtītāja pārziņā esošu personas datus saturošas informācijas aizsardzības pārkāpums, bez nepamatotas kavēšanās, bet ne vēlāk kā 1 (vienas) stundas laikā, paziņot par to Pasūtītājam un veikt visas incidenta novēršanai nepieciešamās darbības. Šī prasība attiecas arī uz piesaistītajiem apakšuzņēmējiem;

2.3.2. incidenta gadījumā vākt un sniegt Pasūtītājam visu informāciju par incidentu, kas var būt noderīga incidenta novēršanai un izmeklēšanai;

2.3.3. nekavējoties, kā kļuvis zināms, informēt par atklātajām piegādātā informācijas un komunikācijas tehnoloģiju produkta vai sniegtā pakalpojuma ievainojamībām, to novēršanas pasākumiem un termiņiem.

**2.4. Piegādātāja pienākumi izstrādājot Pasūtītājam jaunu informācijas sistēmu, veicot esošās informācijas sistēmas izmaiņas, informācijas sistēmas uzturēšanu vai IKT resursu apkopi:**

2.4.1. ne vēlāk kā līdz līguma noslēgšanai par informācijas sistēmas izstrādi, esošās informācijas sistēmas izmaiņām, informācijas sistēmas uzturēšanu vai IKT resursu apkopi iesniedz Pasūtītājam ārpakalpojuma izpildē iesaistīto fizisko personu sarakstu ar skaidrojumu attiecīgās fiziskās personas iesaistei ārpakalpojuma līguma izpildē.

Piegādātājs informē Pasūtītāju par ārpakalpojuma izpildē iesaistīto fizisko personu izmaiņām līguma izpildes laikā;

2.4.2. nepielaist Pakalpojuma izpildei fiziskas personas, kuras, saskaņā ar šo Prasību 2.4.1. apakšpunktu nav rakstiski saskaņotas ar Pasūtītāju;

2.4.3. nodrošināt tiesiskajā darījumā (piemēram, Līgumā) noteikto atjaunošanas punkta mērķi (RPO) un atjaunošanas laika mērķi (RTO);

2.4.4. saglabāt žurnālfailu ierakstus mašīnlasāmā formā atbilstoši informācijas sistēmas drošības klasei, kurai tiek veikts ārpakalpojums. Žurnālfailu glabāšanas termiņš tiek noteikts atbilstoši informācijas sistēmas drošības klasei - A klases informācijas sistēmām: 18 mēnešus; B klases informācijas sistēmām – 12 mēnešus un C klases informācijas sistēmām 6 mēnešus;

2.4.5. informācijas sistēmas rezerves kopijām gan fiziski, gan elektroniskajā vidē var piekļūt Pasūtītāja pilnvarotās personas;

2.4.6. nodrošināt, ka izstrādes gaitā tiek ievērotas Pasūtītāja Kiberdrošības politikā noteiktās prasības. Piegādātājs pieprasa Pasūtītājam iespēju iepazīties ar Kiberdrošības politikas saturu, kas nepieciešams Pakalpojuma sniegšanai;

2.4.7. nodrošināt, ka A un B konfidencialitātes klases informācijas sistēmu testa vidē tiek izmantoti tikai sintētiski dati;

2.4.8. nodrošināt, ka A un B konfidencialitātes klases informācijas sistēmu Pakalpojuma izpilde netiek veikta attiecīgās informācijas sistēmas produkcijas vidē;

2.4.9. nodrošina sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu Pasūtītājam, ne vēlāk kā līdz tiesiskajā darījumā (piemēram, Līgumā) noteiktajam termiņam, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas sistēmā;

2.4.10. nodrošina iespēju turpināt sistēmas ekspluatēšanu ar sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators) jaunākām versijām.

**2.5. Piegādātāja pienākumi nodrošinot iekārtu tai skaitā IKT resursu uzturēšanas darbus. Piegādātājs ievēro šādas vadlīnijas:**

2.5.1. iekārtas uztur saskaņā ar ražotāja ieteiktajiem servisa intervāliem un specifikācijām;

2.5.2. remontdarbus un apkalpošanu veic tikai pilnvarots personāls;

2.5.3. uztur ierakstus (reģistrācijas žurnālu) par visiem bojājumiem, profilaktiskajiem un korektīvajiem apkopes darbiem;

2.5.4. personālam, kas veic tehnisko apkopi, jābūt pietiekami identificētam. Par personām, kuras veic aprīkojuma tehnisko apkopi, uztur ierakstus reģistrācijas žurnālā;

2.5.5. ievēro iekārtu garantijas nosacījumus.

**2.6. Piegādātāja pienākumi veicot Pasūtītāja rīcībā esošo personas datu apstrādi, Piegādātājs ievēro šādus noteikumus:**

2.6.1. Piegādātājs veic personas datu apstrādi tikai tajos gadījumos un tādā apjomā, lai nodrošinātu Pakalpojuma izpildi;

2.6.2. Piegādātājs neizmanto tam pieejamos personas datus no Pakalpojuma neizrietošiem nolūkiem (mērķiem), vai citādi, kā vien saskaņā ar Pasūtītāja rakstveida norādījumiem, ja vien to darīt nepieprasa tiesību akti;

2.6.3. Piegādātājs nodrošina apstrādājamo personas datu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;

2.6.4. Piegādātājs ievēro tehniskās un organizatoriskās personas datu apstrādes aizsardzības prasības, kas noteiktas tiesību aktos. Izvēloties tehniskos un organizatoriskos pasākumus personas datu aizsardzībai, nodrošina personas datu un tehnisko resursu, ar kuriem apstrādā personas datus, aizsardzību pret fiziskās iedarbības radītu personas datu apdraudējumu, kā arī nodrošina ar programmatūras līdzekļiem, parolēm, šifrēšanu un citiem loģiskās aizsardzības līdzekļiem realizētu personas datu aizsardzību;

2.6.5. Piegādātājs nodrošina, ka tā nodarbinātie, kuri ir pilnvaroti apstrādāt personas datus, ir apņēmušies ievērot konfidencialitāti, saglabāt un nelikumīgi neizpaust personas datus, kurus Pasūtītājs nodod Piegādātājam, arī pēc darba vai civildienesta tiesisko attiecību izbeigšanas;

2.6.6. Piegādātājs uztur personas datu apstrādes veikto darbību reģistru un trīs darba dienu laikā pēc pamatota Pasūtītāja pieprasījuma uzrāda to Pasūtītājam;

2.6.7. trīs darba dienu laikā no datu subjekta pieprasījuma par personas datu apstrādi vai tiesību izmantošanas saņemšanas informē par to Pasūtītāju un pēc iespējas palīdz Pasūtītājam ar atbilstīgiem tehniskiem un organizatoriskiem pasākumiem, lai Pasūtītājs varētu atbildēt uz datu subjekta pieprasījumu. Piegādātājs pats nesniedz atbildi uz šo pieprasījumu, ja vien Pasūtītājs to nav atļāvis darīt;

2.6.8. informē Pasūtītāju par datu incidentu (notikums vai nodarījums, kas ir saistīts ar personas datu aizsardzības pārkāpumu, kā arī jebkurš cits kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta personas datu integritāte, pieejamība, konfidencialitāte vai noturība) ne vēlāk kā 1 vienas stundas laikā no brīža, kad incidents Piegādātājam kļuvis zināms, un iespēju robežās sniedz Pasūtītājam atbalstu personas datu aizsardzības pārkāpumu fiksēšanā, incidenta izmeklēšanā un incidenta kaitīgās iedarbības seku novēršanā, ciktāl tas attiecas uz Piegādātāja rīcībā esošo informāciju, kas satur personas datus, un paziņošanu uzraudzības iestādei vai datu subjektam;

2.6.9. tiesību aktos noteiktajos gadījumos pēc valsts vai tiesībsargājošo iestāžu pieprasījuma nodod personas datus valsts, vai tiesībsargājošām iestādēm un trīs darba dienu laikā pēc personas datu nodošanas informē par to Pasūtītāju, izņemot, ja ar normatīvajiem aktiem šāda informēšana ir aizliegta;

2.6.10. neveic datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju bez Pasūtītāja iepriekšēja rakstveida saskaņojuma;

2.6.11. pēc Pakalpojumā noteikto saistību izpildes nodod Pasūtītājam visus personas datus un dzēš kopijas, kas satur personas datus un apliecina Pasūtītājam, ka tas ir izdarīts, ja ir zudis datu apstrādes tiesiskais pamats un tiesību akti neparedz attiecīgo personas datu glabāšanu;

2.6.12. ņemot vērā personas datu apstrādes veidu un Piegādātājam pieejamo informāciju, pēc iespējas sniedz ieteikumus, Pasūtītājam veicot novērtējumu par ietekmi uz personas datu aizsardzību;

2.6.13. sniedz Pasūtītājam nepieciešamo informāciju revīzijas vai pārbaudes veikšanai saistībā ar Pakalpojumā paredzēto pienākumu izpildi;

2.6.14. glabā dokumentus, kas satur personas datus, ievērojot normatīvo tiesību aktu prasības;

2.6.15. atļauj Pasūtītājam iekļūt teritorijā un telpās, kuras Piegādātājs izmanto personas datu apstrādei, Piegādātāja klātbūtnē, lai veiktu attiecīgo personas datu apstrādes darbību

pārbaudi. Piegādātājam ir pienākums nekavējoties informēt Pasūtītāju, ja Datu valsts inspekcija saistībā ar Pasūtītāja personas datu apstrādi uzsāk, vai plāno uzsākt pārbaudi Piegādātāja teritorijā, telpās un/vai informācijas sistēmās;

2.6.16. iespējami ātri atjauno personas datu pieejamību un piekļuvi tiem gadījumā, ja noticis fizisks vai tehnisks negadījums;

2.6.17. nepieciešamības gadījumā izstrādā procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību;

2.6.18. palīdz Pasūtītājam nodrošināt VDAR 32. līdz 36. pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un Piegādātājam pieejamo informāciju;

2.6.19. VDAR 37. pantā noteiktajos gadījumos ir iecēlis vai ieceļ datu aizsardzības speciālistu.

**2.7. Piegādātāja pienākumi Konfidenciālas informācijas apstrādes drošības nodrošināšanā:**

2.7.1. Piegādātājs nodrošina, ka Konfidenciāla informācija netiek izpausta un nav pieejama nevienai trešajai personai, izņemot šo Prasību 4. punkta kārtībā Piegādātāja piesaistīto apakšuzņēmēju tikai tā pienākumu veikšanai nepieciešamajā apjomā, kā arī nodrošina minētās informācijas aizsardzību pret nesankcionētu piekļuvi, nejaušu iznīcināšanu vai noplūdi;

2.7.2. Piegādātājs nodrošina, ka Pasūtītāja infrastruktūrai (IT sistēmām, serveriem un/ vai citām informācijas apstrādes vietām un objektiem), kurā tiek apstrādāta t.sk. glabāta, Konfidenciāla informācija, kā arī šīs informācijas saturam nepiekļūst neviena persona, izņemot Piegādātāju un/vai šo Prasību 4. punktā noteiktā kārtībā Piegādātāja piesaistītā apakšuzņēmēja darbinieki, kuriem piekļuve nepieciešama tiešo pienākumu veikšanai un starp Piegādātāju un Pasūtītāju noslēgtā tiesiskā darījuma izpildei. Tas attiecas gan uz fizisko piekļuvi, gan loģisko piekļuvi (caur informācijas sistēmām), gan piekļuvi dokumentiem papīra formā;

2.7.3. Piegādātājs ir ieviesis un dokumentējis procesu, kas nodrošina iespēju izsekot un noteikt, kurš un kad ir piekļuvis Konfidenciālai informācijai. Tas attiecas gan uz fizisko piekļuvi, gan loģisko piekļuvi (caur informācijas sistēmām), gan piekļuvi dokumentiem papīra formā;

2.7.4. Piegādātājs nodrošina Konfidenciālas informācijas tehnisko aizsardzību, kuru īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem;

2.7.5. Piegādātājs ir noteicis un kontrolē informācijas pārvaldību savā uzņēmumā, kas citu starpā ietver drošības prasības Konfidenciālas informācijas apstrādei;

2.7.6. Piegādātājam ir pienākums pēc savstarpēji noslēgtā tiesiskā darījuma (piemēram, Līguma) termiņa beigām dzēst viņa rīcībā nonākušo Konfidenciālo informāciju, ja vien Pasūtītājs nav noteicis savādāk;

2.7.7. Konfidenciālu informāciju atļauts apstrādāt un glabāt, tai skaitā rezerves kopijās, tikai tādos resursos, kas atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

## 3. Personāla vadības jautājumi

3.1. Piegādātājs ir noslēdzis rakstveida līgumus ar visiem darbiniekiem, kas var piekļūt vai apstrādāt jebkādā veidā Konfidenciālu informāciju. Šajos līgumos Piegādātāja darbinieks ir apņēmies nodrošināt informācijas konfidencialitāti, integritāti, pieejamību un noturību, kā arī

neizpaust iegūto informāciju nenoteiktu laika periodu, t.i., gan darba attiecību laikā, gan pēc darba attiecību izbeigšanas saskaņā ar Piegādātājam saistošajiem Latvijas Republikas normatīvajiem un saistošajiem reglamentējošajiem vai juridiskajiem aktiem, t.sk. līgumiem, kas noslēgti starp Piegādātāju un viņa sniegto pakalpojumu saņēmējiem;

3.2. Pakalpojumu sniegšanā vai saņemšanā Pasūtītājam iesaistītie Piegādātāja darbinieki ir apmācīti datu aizsardzības un informācijas drošības jautājumos;

3.3. Piegādātājs nodrošina, ka Pakalpojumu sniegšanā vai saņemšanā Pasūtītājam iesaistītie tā darbinieki ir informēti, apzinās un ievēro šīs Prasības, uz Pakalpojuma sniegšanu attiecināmos Latvijas Republikā piemērojamos normatīvos aktus (tai skaitā, VDAR), starp Piegādātāju un Pasūtītāju noslēgtā tiesiskā darījuma noteikumus un Pasūtītāja noteiktos informācijas, infrastruktūras un sistēmu izmantošanas noteikumus;

3.4. Piegādātājs informē Pasūtītāju par personāla izmaiņām, kuras saistītas ar pakalpojumu sniegšanu Pasūtītājam un/ vai kuri strādā ar Pasūtītāja informāciju;

3.5. Piegādātājs informē par personas datu nodošanu tos savus Pakalpojuma izpildē iesaistītos nodarbinātos, par kuriem Pakalpojuma izpildes ietvaros nodoti personas dati Pasūtītājam, norādot personas datu apstrādes mērķi, nodoto datu veidus un informējot, ka papildus informācija par to, kā Pasūtītājs apstrādās saņemtos personas datus, ievēros datu aizsardzību un datu subjekta tiesības, ir pieejama pie Pasūtītāja.

## 4. Apakšuzņēmēja piesaistīšana vai nomaiņa

4.1. Piegādātājam ir tiesības piesaistīt jaunu apakšuzņēmēju vai nomainīt apakšuzņēmēju tikai pēc Pasūtītāja rakstiskas piekrišanas saņemšanas, kā arī ievērojot starp Piegādātāju un Pasūtītāju noslēgtā tiesiskā darījuma prasības (ja tādas ir noteiktas). Pirms apakšuzņēmuma piesaistīšanas, Piegādātājs iesniedz Pasūtītājam tās pieprasīto informāciju, kā arī apakšuzņēmēja sniegtu apliecinājumu par atbilstību šīm Prasībām, Latvijas Republikā piemērojamo normatīvo aktu (t.sk, VDAR) prasībām, un citām prasībām, kas ietvertas starp Piegādātāju un Pasūtītāju noslēgtajā tiesiskajā darījumā;

4.2. Piegādātājs uzņemas pilnu atbildību par apakšuzņēmēju, tā darbību un veikto personas datu apstrādi, kā arī sedz jebkāda veida Pasūtītājam radušos zaudējumus šāda apakšuzņēmēja darbības vai bezdarbības rezultātā;

4.3. Piegādātājs nodrošina apakšuzņēmēja informācijas pārvaldības un apstrādes auditu/revīziju pēc Pasūtītāja pieprasījuma Pasūtītāja un Piegādātāja savstarpēji saskaņotā laika periodā, kā arī nodrošina Pasūtītājam iespēju pašam veikt minētā apakšuzņēmēja informācijas pārvaldības un apstrādes auditu/revīziju, nodrošinot iespēju Pasūtītāja pārstāvjiem piekļūt un iepazīties ar dokumentiem, kas pamato apakšuzņēmēja un tā darbības atbilstību Latvijas Republikā piemērojamo normatīvo aktu (tai skaitā, VDAR) prasībām, šīm Prasībām un starp Piegādātāju un Pasūtītāju noslēgtā tiesiskā darījuma prasībām. Pasūtītājs ir atbildīgs par visām izmaksām, kas rodas saistībā ar Pasūtītāja pieprasītajiem auditiem.

5. Ja starp Prasībām un savstarpēji noslēgtā tiesiskā darījuma (piemēram, Līguma) noteikumiem ir pretrunas, piemērojami tie noteikumi, kas nodrošina augstāku informācijas un personas datu aizsardzības līmeni saskaņā ar Pasūtītāja interpretāciju.

Juridiskās un pārvaldes organizācijas

departamenta direktora vietnieks M. Deaks