WORRY FREE IT PLATFORMAS NOTEIKUMI

EIS DARĪJUMIEM

SIA "DATAKOM", reģ. Nr. 40103142605 | Redakcija: 26.10.2026.

1. Vispārīgie noteikumi

1.1. Noteikumi nosaka Worry Free IT Platformas funkcijas, Datakom un pircēja pienākumus un Platformas lietošanas nosacījumus Darījumos, kas noslēgti EIS e-katalogā par Aprakstā norādītajiem Produktiem. Citiem darījumiem Noteikumus nepiemēro.

1.2. Darījumu regulē VV un tās pielikumi. Šie Noteikumi nosaka Platformas lietošanas nosacījumus, Datakom veicamās darbības, Pušu pienākumus un Datakom atbildības robežas. Samaksas, piegādes un pieņemšanas kārtību, līgumsodus, atkāpšanos no Darījuma, nepārvaramu varu un strīdu risināšanu regulē VV.

1.3. Apraksts un Noteikumi ir publicēti Tīmekļvietnē. EIS Preces kartītes laukā "Apraksts" ir saite uz Aprakstu, savukārt Aprakstā ir saite uz Noteikumiem. Apstiprinot pirkuma pasūtījumu par Produktu, pircējs apliecina piekrišanu Noteikumiem. Atsevišķa Noteikumu parakstīšana nav nepieciešama.

1.4. Darījumam piemēro to Noteikumu un Apraksta redakciju, kas bija publicēta Tīmekļvietnē pirkuma pieprasījuma izveides dienā. Datakom Tīmekļvietnē saglabā iepriekšējās redakcijas un to publicēšanas datumus, lai būtu iespējams noteikt konkrētajam Darījumam piemērojamos dokumentus. Vēlāk publicēti grozījumi noslēgtu Darījumu nemaina, ja vien Puses nav vienojušās citādi VV noteiktajā kārtībā.

1.5. Ja Darījuma dokumenti ir savstarpēji pretrunā, tos piemēro šādā prioritārā secībā: 1) VV un tās pielikumi; 2) EIS noformētais pirkuma pasūtījums, tostarp tajā norādītie un Datakom piedāvājumā pieņemtie nosacījumi, komentāri un pievienotās datnes; 3) Noteikumi; 4) Apraksts. Pircēja vienpusēji pievienoti nosacījumi, kurus Datakom nav pieņēmis VV noteiktajā kārtībā, paši par sevi nemaina Datakom saistības.

2. Termini

2.1. **Abonements** - pircēja tiesības 12 mēnešus lietot Platformu un Datakom pienākums šajā laikā veikt Produktā iekļautās darbības.

2.2. **Apraksts** - Worry Free IT produktu grupas apraksts EIS darījumiem.

2.3. **Atrisināšanas mērķa laiks** - plānotais laiks Pieteikuma atrisināšanai vai darbības atjaunošanai. Tas ir mērķrādītājs, nevis saistošs termiņš.

2.4. **Darbdiena** - diena, kas nav sestdiena, svētdiena vai Latvijas Republikā noteikta svētku diena.

2.5. **Darījums** - VV noteiktajā kārtībā EIS noslēgts iepirkuma līgums par Produktu.

2.6. **Datakom** - SIA "DATAKOM", reģistrācijas Nr. 40103142605, Platformas ražotājs un piegādātājs VV izpratnē.

2.7. **Drošības incidents** - notikums vai notikumu kopums, kas apdraud vai var apdraudēt informācijas konfidencialitāti, integritāti, pieejamību, autentiskumu vai IT infrastruktūras drošu darbību.

2.8. **EIS** - Elektronisko iepirkumu sistēma.

2.9. **Iegādes vienība** - viena lietotāja vai viena servera Abonements uz 12 mēnešiem. Iegādes vienības skaits atbilst lietotāju un serveru kopskaitam, par kuru Puses vienojušās Darījumā.

2.10. **Incidents** - neplānots notikums, kas traucē vai pasliktina IT infrastruktūras darbību un ko pēc ietekmes klasificē kā P1, P2, P3 vai P4 prioritātes Pieteikumu.

2.11. **Infrastruktūras apraksts** - pircēja IT resursu apraksts, kura saturs noteikts Aprakstā un ko pircējs pievieno pirkuma pieprasījumam.

2.12. **IT infrastruktūra** - Pārvaldības apjomā iekļautās pircēja galiekārtas, serveri, programmatūra, lietotāju konti, mākoņpakalpojumi, tīkla iekārtas un citi informācijas tehnoloģiju resursi.

2.13. **MDM** - mobilo ierīču pārvaldības risinājums (Mobile Device Management).

2.14. **Papildu darbi** - darbi, kas neietilpst Platformas funkcijās vai pārsniedz Pārvaldības apjomu.

2.15. **Pārvaldības apjoms** - pircēja IT resursu skaits un sastāvs, kas norādīts Infrastruktūras aprakstā, ietverts Datakom pieņemtajā piedāvājumā un fiksēts Platformas uzskaitē.

2.16. **Pieteikums** - pieteikumu sistēmā reģistrēts pircēja lietotāja pieprasījums, kas iesniegts 7.8. punktā noteiktajā kārtībā, vai Datakom paša konstatēts Incidents.

2.17. **Pircēja kontaktpersona** - pircēja norādīta persona, kas iesniedz P1 Pieteikumus un izmaiņu pieprasījumus, saņem tehniskus paziņojumus un sniedz tehniskus apstiprinājumus.

2.18. **Pircējs** - pasūtītājs, kas EIS iegādājas vai ir iegādājies Produktu.

2.19. **Pirkuma pasūtījums** - pircēja apstiprināts pirkuma pieprasījums.

2.20. **Pirkuma pieprasījums** - pircēja EIS izveidots piedāvājums slēgt Darījumu par Produktu.

2.21. **Platforma** - Worry Free IT risinājums, ar kuru Datakom nodrošina Platformas funkcijas. To veido programmatūra, mākoņrīki, RMM, drošības rīki, pieteikumu sistēma un Datakom darbības.

2.22. **Platformas aktivizēšana** - brīdis, kad Datakom paziņo pircēja kontaktpersonai, ka Platforma darbojas Pārvaldības apjomā.

2.23. **Platformas funkcijas** - Noteikumu 4. nodaļā noteiktās darbības.

2.24. **Platformas uzskaite** - Datakom uzturēts Pārvaldības apjomā iekļauto resursu saraksts.

2.25. **Plānotie darbi** - iepriekš saskaņotas izmaiņas vai citi plānoti darbi, ko klasificē kā P5 prioritātes Pieteikumu.

2.26. **Preces kartīte** - Produkta ieraksts EIS e-katalogā.

2.27. **Produkts** - Worry Free IT produktu grupas produkts ar savu kodu. Produkti, to SLA līmeņi un Trešo personu komponentes ir norādīti Aprakstā.

2.28. **Puses** - pircējs un Datakom.

2.29. **Reakcijas laiks** - laiks no pilnīga Pieteikuma saņemšanas līdz Datakom pirmajai atbildei, kurā norādīts Pieteikuma numurs un nākamā darbība.

2.30. **RMM** - attālinātās uzraudzības un pārvaldības risinājums (Remote Monitoring and Management), tostarp tā aģenti pircēja iekārtās.

2.31. **Servisa pieprasījums** - standarta pieprasījums, kas nav saistīts ar darbības traucējumu un ko klasificē kā P4 prioritātes Pieteikumu, piemēram, konta izveide, piekļuves piešķiršana vai konfigurācijas maiņa.

2.32. **SLA** - Noteikumu 7. nodaļā noteiktie atbalsta līmeņa rādītāji (Service Level Agreement).

2.33. **SLA līmenis** - Standard, Extended vai Premium.

2.34. **SLA pieejamības laiks** - laiks, kurā skaita Reakcijas laiku un Atrisināšanas mērķa laiku.

2.35. **Tīmekļvietne** - Datakom tīmekļvietnes lapa https://www.datakom.lv/lv/worry-free-it-noteikumi/, kurā publicēti Apraksts, Noteikumi un to iepriekšējās redakcijas.

2.36. **Trešo personu komponentes** - programmatūra, mākoņrīki, saskarnes (API) un citi tehnoloģiskie risinājumi, ko izmanto Platformā un ko piegādā vai kontrolē trešā persona.

2.37. **VDAA** - Valsts digitālās attīstības aģentūra.

2.38. **VV** - VDAA vispārīgā vienošanās ar pielikumiem, kuras e-katalogā pircējs iegādājies Produktu. Aktuālā VV un e-kataloga pozīcija ir norādītas Aprakstā.

3. Produkts, Abonements un Platformas aktivizēšana

3.1. Produkta kods nosaka SLA līmeni un Produktā iekļautās Trešo personu komponentes. Platformas pamatfunkcijas ir vienādas visiem Produktiem, bet atsevišķu funkciju pieejamība ir atkarīga no konkrētajā Produktā iekļautajām komponentēm un Noteikumos norādītajiem priekšnosacījumiem, tostarp 4.3.4. un 4.5.3. punktā.

3.2. Pircējs pirkuma pieprasījumā norāda Iegādes vienību skaitu, komentārā norāda izvēlētā Produkta kodu (VV 3. pielikuma 1.4.1. punkts) un pievieno Infrastruktūras aprakstu. Datakom sagatavo piedāvājumu par tajā noteikto Pārvaldības apjomu VV 1.8. punktā un 3. pielikuma 1.5. punktā paredzētajā kārtībā.

3.3. Lietotāja Iegādes vienībā ietilpst šā lietotāja konti un viņa lietotās darbstacijas un mobilās ierīces, kas norādītas Infrastruktūras aprakstā un iekļautas saskaņotajā Pārvaldības apjomā. Tīkla iekārtām un citiem Infrastruktūras aprakstā norādītajiem resursiem atsevišķa Iegādes vienība nav nepieciešama, tomēr to pārvaldība attiecas tikai uz piedāvājumā saskaņoto resursu skaitu un sastāvu.

3.4. Ja pircējs Abonementa termiņā vēlas palielināt Pārvaldības apjomu, tas EIS izveido jaunu pirkuma pieprasījumu par papildu apjomu. Pārvaldības apjoma samazināšanās pati par sevi nemaina jau noslēgtā Darījuma cenu.

3.5. Datakom reizi ceturksnī salīdzina Platformas uzskaiti ar saskaņoto Pārvaldības apjomu un informē pircēju par resursiem, kuri pārsniedz šo apjomu. Šādus resursus Datakom iekļauj pārvaldībā pēc tam, kad par papildu apjomu VV noteiktajā kārtībā ir noformēts jauns pirkuma pasūtījums.

3.6. Abonements ilgst 12 mēnešus no Platformas aktivizēšanas. Atjaunots Abonements ilgst 12 mēnešus no 3.11. punktā noteiktās dienas.

3.7. Datakom aktivizē Platformu 20 Darbdienu laikā pēc Darījuma noslēgšanas (VV 3. pielikuma 2.3. punkts). Aktivizēšanas laikā Datakom veic Aprakstā noteiktos ieviešanas darbus, tostarp izveido pircēja vidi Platformā, uzstāda RMM aģentus vai nodod tos pircējam uzstādīšanai, sākotnēji uzskaita pārvaldībā iekļautos resursus un piešķir pircēja kontaktpersonām piekļuvi pieteikumu sistēmai.

3.8. Ja Platformas aktivizēšanu kavē pircēja nenodrošināta piekļuve, informācija vai 6.6. punktā paredzētās licences, Puses vienojas par piegādes termiņa pagarinājumu VV noteiktajā kārtībā.

3.9. Pircējs pārbauda Platformas darbību un EIS apstiprina tās kvalitāti piecu Darbdienu laikā pēc Platformas aktivizēšanas (VV 3. pielikuma 2.4. punkts).

3.10. Pēc Platformas kvalitātes apstiprināšanas pircējs iegūst neekskluzīvas un tālāk nenodotamas tiesības Abonementa termiņā lietot Platformas programmatūru savām vajadzībām. Īpašuma tiesības uz programmatūru un tās pirmkodu pircējam nepāriet.

3.11. Lai atjaunotu Abonementu, pircējs EIS izveido jaunu pirkuma pieprasījumu un komentārā norāda esošā Abonementa beigu datumu (VV 3. pielikuma 1.4.2. punkts). Ja jaunais Darījums noslēgts pirms esošā Abonementa beigām, atjaunotais Abonements sākas nākamajā dienā pēc esošā Abonementa beigām, un 3.7. punktā noteikto atkārtotas aktivizēšanas kārtību nepiemēro.

3.12. Samaksu veic VV noteiktajā kārtībā. Ikmēneša rēķinus piemēro, ja pircējs to norāda pirkuma pieprasījuma komentārā (VV 3. pielikuma 2.6. punkts).

4. Platformas funkcijas

4.1. Šajā nodaļā izsmeļoši noteiktas Platformas funkcijas un to piemērošanas nosacījumi. Datakom tās nodrošina tikai saskaņotajā Pārvaldības apjomā un ar Produktā pieejamajām komponentēm.

4.2. **IT infrastruktūras uzskaite**

4.2.1. Datakom izveido un uztur Platformas uzskaiti un aktualizē to pēc pircēja paziņotajām vai Datakom konstatētajām izmaiņām.

4.2.2. Datakom uztur IT infrastruktūras tehnisko dokumentāciju tādā apjomā, kāds nepieciešams Platformas funkcijām.

4.3. **IT infrastruktūras uzturēšana**

4.3.1. Datakom uzrauga IT infrastruktūras veiktspēju un sniedz ieteikumus tās uzlabošanai. Ja veiktspējas traucējumu var novērst Platformas funkciju robežās, Datakom to novērš. Ja nepieciešami Papildu darbi, Datakom par to informē pircēju.

4.3.2. Datakom pārvalda pretvīrusu aizsardzības (AV) un galiekārtu apdraudējumu atklāšanas un reaģēšanas (EDR) risinājumus: pārbauda to darbības statusu, novērš ar Platformas rīkiem konstatējamās kļūdas un pēc nepieciešamības koriģē drošības politikas.

4.3.3. Datakom Platformas tehnisko iespēju robežās konstatē IT infrastruktūras kiberdrošības riskus un reaģē uz identificētajiem apdraudējumiem.

4.3.4. Datakom pārskata un atjaunina e-pasta drošības filtrus. Ja konkrētajā Produktā ietilpst Nimblr, Datakom papildus nodrošina pircēja lietotājiem automatizētas pikšķerēšanas simulācijas un tiešsaistes drošības apmācību moduļus.

4.3.5. Datakom pēc pircēja pieprasījuma izskata lūgumus piemērot izņēmumus drošības prasībām, pārskata jau apstiprinātos izņēmumus un aktualizē ar tiem saistīto risku novērtējumu.

4.3.6. Datakom izvērtē un instalē programmatūras un serveru programmaparatūras atjauninājumus. Datakom uzrauga kritiskās ievainojamības, tostarp nulles dienas ievainojamības, un uzstāda drošības labojumus, ja ražotājs tos ir izlaidis un uzstādīšana ir tehniski iespējama.

4.3.7. Datakom var uzstādīt un atjaunināt pircēja izmantoto trešo personu programmatūru, ja tā atbilst Platformas drošības un savietojamības prasībām. Ja programmatūra nav atbalstāma vai rada būtisku drošības, savietojamības vai uzturēšanas risku, Datakom var atteikties to uzturēt un par to informē pircēju, norādot iemeslu. Ja pircējs šādu programmatūru turpina lietot, tās izraisīto traucējumu un Drošības incidentu novēršana neietilpst Platformas funkcijās.

4.4. **Rezerves kopēšanas uzraudzība**

4.4.1. Ja Infrastruktūras aprakstā norādīts pircēja rezerves kopēšanas risinājums, kas spēj nodot Platformai rezerves kopēšanas uzdevumu izpildes statusu, Datakom uzrauga šo statusu Pārvaldības apjomā iekļautajām iekārtām, serveriem un mākoņpakalpojumiem.

4.4.2. Datakom veic konfigurācijas izmaiņas, kas nepieciešamas rezerves kopēšanas uzdevumu izpildes statusa saņemšanai. Ja uzdevums nav izpildīts vai ir izpildīts ar kļūdām, Datakom novērš kļūdu tiktāl, ciktāl to iespējams izdarīt ar Platformas rīkiem.

4.4.3. Rezerves kopēšanas uzraudzība neietver rezerves kopēšanas risinājuma ieviešanu, datu atjaunošanas testēšanu, rezerves kopiju integritātes pārbaudi un datu atjaunošanu. Datakom neuzņemas pienākumu nodrošināt rezerves kopiju izveidi, pilnīgumu vai iespēju no tām atjaunot datus.

4.5. **Identitāšu un mobilo ierīču pārvaldība**

4.5.1. Datakom pārvalda e-pasta un lietotāju kontus, konfigurē daudzfaktoru autentifikāciju (MFA), ievieš un uztur identitātes drošības politikas.

4.5.2. Datakom pārvalda lietotāju piekļuves tiesības, pārbauda piekļuves noteikumus, daudzfaktoru autentifikācijas piemērošanu lietotāju kontiem un identitātes pārvaldības sistēmas drošības iestatījumus, kā arī sniedz ieteikumus.

4.5.3. Ja Infrastruktūras aprakstā ir norādītas mobilās ierīces, Datakom pārvalda tās ierīces, kuras pircējs nodevis pārvaldībā un kuras ir reģistrētas MDM risinājumā. Datakom ierīces reģistrē un uzskaita, konfigurē pircēja apstiprinātās drošības politikas, pārbauda atbilstības statusu, izvieto lietotnes un konfigurē piekļuves nosacījumus pircēja resursiem. MDM licences pircējs nodrošina 6.6. punktā noteiktajā kārtībā.

4.6. **Tīkla iekārtu pārvaldība**

4.6.1. Ja Infrastruktūras aprakstā ir norādītas tīkla iekārtas, Datakom atjaunina ugunsmūru, maršrutētāju, komutatoru, Wi-Fi kontrolieru un bezvadu piekļuves punktu programmaparatūru, ja atjauninājumi ir pieejami un attiecīgajām iekārtām tehniski piemērojami.

4.6.2. Datakom veido tīkla iekārtu konfigurāciju rezerves kopijas un pārbauda to integritāti Platformas tehnisko iespēju robežās.

4.6.3. Datakom uztur tīkla iekārtu uzskaiti.

4.7. **Pārskati un konsultācijas**

4.7.1. Datakom katru mēnesi sagatavo pārskatu par Incidentiem, Reakcijas laika ievērošanu, Atrisināšanas mērķa laika sasniegšanu, uzraudzības rezultātiem, drošības notikumiem un būtiskākajiem ieteikumiem.

4.7.2. Datakom reizi ceturksnī sagatavo Platformas funkciju izpildes un IT attīstības pārskatu (Quarterly Business Review, QBR), izmantojot Platformas uzskaitē, pieteikumu sistēmā un citos Platformas rīkos pieejamo informāciju.

4.7.3. Datakom sagatavo un aktualizē IT attīstības plānu turpmākajiem 12 līdz 24 mēnešiem, izmantojot Platformā pieejamo informāciju un pircēja sniegtos darbības un IT attīstības plānus. Jaunas IT infrastruktūras projektēšana un detalizētu ieviešanas projektu izstrāde ir Papildu darbi.

4.7.4. Datakom pēc nepieciešamības sniedz konsultācijas informācijas drošības jautājumos un pārskata ar Pārvaldības apjomu saistītās IT politikas un procesus. Padziļināti auditi un atbilstības nodrošināšanas projekti neietilpst Platformas funkcijās.

4.7.5. Datakom uztur uzskaiti par savā pārvaldībā esošajām programmatūras licencēm un abonementiem, tostarp to atjaunošanas termiņiem.

4.8. **Atbalsts**

4.8.1. Datakom reģistrē, klasificē un risina Incidentus atbilstoši 7. nodaļai.

4.8.2. Datakom izpilda Servisa pieprasījumus Platformas funkciju un Pārvaldības apjoma robežās, tostarp izveido lietotāju kontus, piešķir piekļuves tiesības un veic standarta konfigurācijas izmaiņas.

4.8.3. Datakom konsultē pircēja lietotājus par Pārvaldības apjomā iekļautajām operētājsistēmām, biroja programmatūru un iekārtām.

4.8.4. Datakom sniedz atbalstu latviešu un angļu valodā visos 7.8. punktā noteiktajos kanālos. Ja Datakom atbalstā iesaista apakšuzņēmēju, arī tas sniedz atbalstu šajās valodās. Atbalstu citās valodās Datakom sniedz tikai pēc atsevišķas vienošanās.

4.8.5. Ja Incidentu vai Servisa pieprasījumu nevar atrisināt attālināti, Datakom veic nepieciešamos darbus klātienē Infrastruktūras aprakstā norādītajās adresēs. Klātienes darbu un transporta izmaksas, arī braucieniem uz adresēm, kas atrodas tālāk par 30 km no Datakom biroja Malduguņu ielā 2, Mārupē, ir iekļautas piedāvājuma cenā, un Datakom tās atsevišķi neaprēķina.

4.9. Ja Noteikumos nav noteikts konkrētas darbības biežums, Datakom to nosaka, ņemot vērā Pārvaldības apjomu, tehniskos riskus un profesionālo praksi. Datakom plāno ievainojamību pārskatu reizi mēnesī un AV un EDR darbības statusa pārbaudi reizi nedēļā. Šis biežums nav SLA rādītājs.

4.10. Datakom Platformas funkcijas nodrošina ar profesionālu rūpību. Platformas izmantošana pati par sevi negarantē IT infrastruktūras darbību bez traucējumiem, pilnīgu aizsardzību pret kiberdraudiem vai noteiktu darbības nepārtrauktības, audita vai normatīvās atbilstības rezultātu.

5. Darbības, kas neietilpst Platformas funkcijās

5.1. Platformas funkcijās neietilpst:

- jaunas IT infrastruktūras projektēšana un ieviešana, tostarp jaunu serveru, tīkla vai drošības risinājumu ieviešana
- aparatūras fiziska uzstādīšana, pārvietošana vai nomaiņa
- pielāgotas programmatūras izstrāde
- padziļināta digitālā incidentu izmeklēšana, izņemot 7. nodaļā paredzēto Incidentu apstrādi
- lietotāju klātienes apmācību organizēšana
- trešo personu programmatūras ražotāja kļūdu novēršana un ražotāja tehniskā atbalsta aizstāšana
- darbības atsevišķu normatīvo prasību izpildei, ja tās nav paredzētas Noteikumos
- fiziskās drošības un telekomunikāciju infrastruktūras apkope

5.2. Papildu darbus pircējs var iegādāties atsevišķā EIS darījumā Aprakstā norādītajā e-kataloga pozīcijā. Uz šiem darbiem attiecas attiecīgā vispārīgā vienošanās un darba uzdevums, nevis šie Noteikumi.

5.3. Ja pircēja pieprasītā darbība neietilpst Platformas funkcijās vai pārsniedz Pārvaldības apjomu, Datakom pirms darba sākšanas par to informē pircēja kontaktpersonu.

6. Pircēja sadarbība

6.1. Pircējs pirkuma pieprasījuma komentārā vai Platformas aktivizēšanas laikā norāda kontaktpersonas. Bez atsevišķa pilnvarojuma pircēja kontaktpersonas nav tiesīgas grozīt Darījumu.

6.2. Pircējs nodrošina Datakom savlaicīgu un drošu piekļuvi Pārvaldības apjomā iekļautajām sistēmām un sniedz informāciju, kas nepieciešama Platformas funkcijām.

6.3. Pircējs lieto ražotāju atbalstītas iekārtu un programmatūras versijas. Ja Datakom ir informējis pircēju, ka tehnoloģija nav atbalstīta, tās izraisīto traucējumu un Drošības incidentu novēršana neietilpst Platformas funkcijās.

6.4. Pircējs nekavējoties informē Datakom par izmaiņām IT infrastruktūrā, lietotāju kontos, piekļuves tiesībās, tīklā, mākoņpakalpojumos un citos apstākļos, kas var ietekmēt Platformas funkcijas, drošību vai Pārvaldības apjomu, kā arī par nozaudētām vai nozagtām pārvaldītajām ierīcēm. Tīkla iekārtu konfigurāciju un tīkla piekļuves noteikumus pircējs maina, iepriekš saskaņojot ar Datakom.

6.5. Pircējs nosaka kritiskos datus, datu atjaunošanas punkta mērķi (RPO) un darbības atjaunošanas laika mērķi (RTO), organizē lietotāju informēšanu un klātienes apmācības, kā arī nodrošina IT infrastruktūras fizisko drošību.

6.6. Licences

6.6.1. Pircējs Platformas aktivizēšanas brīdī un visā Abonementa termiņā nodrošina spēkā esošas Microsoft licences ar šādām funkcijām:

- Microsoft Intune Plan 1 vai plašākas funkcijas ierīču un lietotņu centralizētai pārvaldībai
- Microsoft Entra ID P1 vai plašākas funkcijas identitātes un piekļuves pārvaldībai, tostarp ar pārvaldītajām ierīcēm saistītām piekļuves politikām

6.6.2. Šīs funkcijas var nodrošināt ar vienu Microsoft licences plānu vai vairāku licenču kombināciju, piemēram, ar Microsoft 365 Business Premium, Microsoft 365 E3 vai E5, Enterprise Mobility + Security E3 vai E5 vai ar Microsoft Intune Plan 1 kopā ar Microsoft Entra ID P1. Noteicošā ir nepieciešamo funkciju un atbilstošu lietošanas tiesību esība, nevis konkrēta licences plāna nosaukums.

6.6.3. Pircējs nodrošina licences visiem lietotājiem un ierīcēm, uz kuriem šīs funkcijas attiecas, atbilstoši Microsoft licencēšanas noteikumiem.

6.6.4. Ja kādai Platformas funkcijai nepieciešama licence, kas nav minēta 6.6.1.-6.6.5. punktā, Datakom par to informē pircēju pirms funkcijas ieviešanas. Ja pircējs šādu licenci nenodrošina, piemēro 6.6.7. punktu.

6.6.5. Samsung ierīču reģistrēšanai un konfigurēšanai Datakom izmanto Samsung bezmaksas rīkus Knox Mobile Enrollment un Knox Platform for Enterprise. Ja pircējs vēlas izmantot maksas

Samsung Knox Suite funkcijas, piemēram, Knox Manage vai Knox E-FOTA, pircējs nodrošina attiecīgās licences.

6.6.6. Pircējs nodrošina arī citu programmatūras un mākoņpakalpojumu licences, kas nav Produkta Trešo personu komponentes.

6.6.7. Ja nepieciešamo licenču nav vai to lietošanas tiesības nav pietiekamas, Datakom attiecīgo funkciju nenodrošina, un tās izpildei SLA nepiemēro līdz brīdim, kad pircējs ir nodrošinājis vajadzīgās licences.

6.7. Datakom un pircēja pienākumu sadalījums apkopots Noteikumu pielikumā. Ja pielikuma tabulas formulējums atšķiras no konkrētā Noteikumu punkta, piemēro attiecīgo Noteikumu punktu.

7. SLA un Pieteikumi

7.1. SLA līmeni nosaka Produkts. SLA pieejamības laiks ir šāds:

SLA līmenis	SLA pieejamības laiks
Standard	Darbdienās no plkst. 9.00 līdz 18.00 visām prioritātēm.
Extended	P1 prioritātei - visu diennakti, septiņas dienas nedēļā. P2-P4 prioritātei - Darbdienās no plkst. 9.00 līdz 18.00.
Premium	P1-P4 prioritātei - visu diennakti, septiņas dienas nedēļā.

7.2. Reakcijas laiku un Atrisināšanas mērķa laiku aprēķina tikai attiecīgajai prioritātei noteiktajā SLA pieejamības laikā.

7.3. Platformas drošības rīki uz apdraudējumiem reaģē automātiski visu diennakti, piemēram, izolē iekārtu vai bloķē ļaunprogrammatūru. Datakom speciālisti reaģē atbilstoši SLA līmenim.

7.4. Pieteikumus iedala Incidentos (P1-P3), Servisa pieprasījumos (P4) un Plānotajos darbos (P5):

Prioritāte	Reakcijas laiks	Atrisināšanas mērķa laiks	Raksturojums	Piemēri
P1 Kritisks	15 minūtes	4 stundas	Pilnīgs IT sistēmu pārtraukums, kas skar visus vai lielāko daļu lietotāju, vai kritisks Drošības incidents ar būtisku ietekmi.	Servera kļūme, e-pasta sistēmas pārtraukums, izspiedējvīruss.
P2 Augsts	1 stunda	8 stundas	Būtisks traucējums, kas skar vairākus lietotājus vai kritisku darbības procesu, tostarp objektīvi konstatējams būtisks veiktspējas kritums.	VPN kļūme, koplietojama printera darbības pārtraukums, būtiski palēnināta sistēmu darbība.
P3 Vidējs	4 stundas	24 stundas	Traucējums, kas skar vienu lietotāju vai nekritisku funkciju.	Viena lietotāja datora problēma, programmatūras kļūda.
P4 Zems	8 stundas	48 stundas	Informācijas vai standarta konfigurācijas pieprasījums, neliels uzlabojums vai cita nekritiska darbība.	Jauna konta izveide, paroles maiņa, konfigurācijas pieprasījums.
P5 Plānotie darbi	Nav	Nav	Iepriekš saskaņoti darbi vai izmaiņas.	Saskaņota izmaiņa.

7.5. Datakom, ņemot vērā traucējuma faktisko ietekmi un steidzamību, nosaka Pieteikuma galīgo prioritāti un par tās maiņu informē pircēju, norādot pamatojumu.

7.6. Reakcijas laika ievērošana ir Datakom pienākums. Datakom pirmajā atbildē norāda Pieteikuma numuru un nākamo darbību.

7.7. Atrisināšanas mērķa laiks ir kvalitātes mērķrādītājs, nevis garantēts Incidenta vai Servisa pieprasījuma atrisināšanas termiņš. Tā sasniegšanu var ietekmēt trešo personu darbības, garantijas remonts, rezerves

daļu vai aparatūras pieejamība, pircēja reakcijas laiks, piekļuves vai informācijas trūkums un citi no Datakom neatkarīgi apstākļi.

7.8. Pircēja lietotāji Pieteikumus iesniedz:

7.8.1. Datakom pieteikumu sistēmā (klientu portālā);

7.8.2. pa e-pastu support@datakom.lv;

7.8.3. pa tālruni +371 67 442 800. P1 Pieteikumu iesniedz tikai pa tālruni.

7.9. P1 Pieteikumus un izmaiņu pieprasījumus iesniedz tikai pircēja kontaktpersonas.

7.10. Ja lietotājs P2, P3 vai P4 Pieteikumu iesniedz pa e-pastu, bet 15 minūšu laikā nesaņem automātisku apstiprinājumu par tā reģistrēšanu, lietotājs atkārtoti piesaka Pieteikumu pa tālruni. Ja e-pasts nosūtīts ārpus attiecīgā SLA pieejamības laika, 15 minūšu termiņu skaita no nākamā SLA pieejamības perioda sākuma. Ja Datakom sistēmas darbības traucējumu dēļ apstiprinājums nav nosūtīts, bet ir iespējams objektīvi pierādīt, ka Pieteikums sasniedzis Datakom norādīto e-pasta adresi, to uzskata par saņemtu tā faktiskās saņemšanas brīdī. Pretējā gadījumā līdz Pieteikuma reģistrēšanai vai telefoniskai pieteikšanai SLA termiņu neaprēķina.

7.11. Datakom reģistrē Pieteikumu 15 minūšu laikā pēc tā saņemšanas attiecīgajā SLA pieejamības laikā. Par saņemšanas brīdi uzskata Pieteikuma automātiskās izveides brīdi pieteikumu sistēmā, zvana reģistrēšanas brīdi vai pierādāmu e-pasta saņemšanas brīdi 7.10. punktā paredzētajā gadījumā. Klientu portālā iesniegts Pieteikums uzskatāms par saņemtu tā reģistrēšanas brīdī.

7.12. SLA termiņus sāk skaitīt no pilnīga Pieteikuma saņemšanas attiecīgajā SLA pieejamības laikā. Ja Pieteikums saņemts ārpus šā laika, termiņus sāk skaitīt nākamā SLA pieejamības perioda sākumā. Pieteikums ir pilnīgs, ja tas satur informāciju, kas objektīvi nepieciešama tā apstrādes sākšanai. Ja būtiskas informācijas trūkst, Datakom bez nepamatotas kavēšanās lūdz to precizēt.

7.13. Saziņa citos kanālos, piemēram, WhatsApp vai Microsoft Teams tērzēšanā, nav Pieteikums, ja Datakom to nav reģistrējis pieteikumu sistēmā.

7.14. Datakom nodrošina pircēja kontaktpersonām piekļuvi pieteikumu sistēmai, lai tās varētu sekot Pieteikumu izskatīšanas gaitai.

7.15. SLA termiņos neieskaita dokumentētu laiku, kad Datakom gaida pircēja darbību, informāciju vai piekļuvi, kā arī laiku, kad traucējuma cēlonis ir ārpus Datakom ietekmes un Datakom ir veicis saprātīgi nepieciešamās darbības tā ietekmes mazināšanai. Plānotās apkopes laiku neieskaita saskaņā ar 8.4. punktu.

7.16. Incidentus, kurus Datakom konstatē pats, piemēram, saņemot RMM vai EDR brīdinājumu, Datakom reģistrē kā Pieteikumus un klasificē pēc 7.4. punktā noteiktajiem kritērijiem. SLA termiņus skaita no Pieteikuma reģistrēšanas brīža attiecīgajā SLA pieejamības laikā.

7.17. P1 Incidenta risināšanas laikā Datakom norīko incidenta vadītāju, 15 minūšu laikā pēc Pieteikuma saņemšanas vai reģistrēšanas sazinās ar pircēja kontaktpersonu un sniedz aktuālu informāciju līdz darbības atjaunošanai vai pircējam pieņemama pagaidu risinājuma ieviešanai. Šo pienākumu izpilda atbilstoši attiecīgā SLA līmeņa pieejamības laikam.

7.18. Pēc P1 Incidenta atrisināšanas Datakom piecu Darbdienu laikā iesniedz pircējam incidenta pēcanalīzes ziņojumu (Post-Incident Report, PIR) ar notikuma aprakstu, cēloņu analīzi un informāciju par veiktajiem pagaidu vai pastāvīgajiem labojumiem. Par P2 Incidentu pircējs var pieprasīt šādu ziņojumu, ko Datakom iesniedz 10 Darbdienu laikā, ja vien analīzei nepieciešamā trešās personas iesaiste nepamato ilgāku termiņu.

7.19. Pēc Pieteikuma izpildes Datakom par to paziņo Pieteikuma iesniedzējam. Ja 72 stundu laikā pircējs nav iesniedzis pamatotus iebildumus, Pieteikums SLA uzskaitē uzskatāms par atrisinātu. Darījuma pieņemšanu regulē VV.

7.20. Datakom ikmēneša pārskatā norāda faktisko Reakcijas laiku un Pieteikumu atrisināšanas laiku, Reakcijas laika ievērošanas īpatsvaru un Atrisināšanas mērķa laika sasniegšanas īpatsvaru. Katru īpatsvaru aprēķina, attiecīgajā mēnesī noteiktajā laikā apstrādāto attiecīgās kategorijas Pieteikumu skaitu dalot ar

visu šīs kategorijas Pieteikumu skaitu, kuriem attiecīgais termiņš ir aprēķināms. Ja nav neviena šāda Pieteikuma, īpatsvaru norāda kā nepiemērojamu. Termiņu aprēķinā ievēro 7.2., 7.12. un 7.15. punktu.

7.21. Ja Datakom bez objektīvi pamatota iemesla nav ievērojis saistošo Reakcijas laiku, pircējs 15 dienu laikā pēc ikmēneša pārskata saņemšanas var iesniegt rakstveida pretenziju. Ja pretenzija ir pamatota, Datakom piemēro samērīgu atlaidi līdz 10 % no Abonementa maksas par attiecīgo mēnesi, ņemot vērā kavēto Pieteikumu skaitu, kavējuma ilgumu un faktisko ietekmi uz pircēju. Abonementa mēneša maksa ir viena divpadsmitā daļa no Darījuma cenas. Atlaidi ņem vērā, aprēķinot līgumsodu vai zaudējumu atlīdzību par vienu un to pašu pārkāpumu, nepieļaujot dubultu atlīdzināšanu. SLA rādītāju neizpilde pati par sevi nav piegādes vai garantijas saistību nokavējums VV 2. pielikuma 5.3.1. punkta izpratnē.

7.22. Būtiska pārkāpuma esību izvērtē saskaņā ar VV 2. pielikuma 7.2. punktu. Šādā izvērtējumā īpaši ņem vērā gadījumu, kad Reakcijas laika ievērošanas īpatsvars bez objektīva pamatojuma divus secīgus mēnešus ir zemāks par 85 %. Atrisināšanas mērķa laika nesasniegšana pati par sevi nav būtisks pārkāpums, jo šis laiks ir nesaistošs mērķrādītājs. Tā sasniegšanu Datakom atspoguļo ikmēneša pārskatā (7.20. punkts).

7.23. Datakom speciālistu reaģēšanas pienākumu ārpus Darbdienām un darba laika nosaka izvēlētais SLA līmenis atbilstoši 7.1. punktam. Ārpus attiecīgā SLA pieejamības laika Datakom var pēc saviem ieskatiem sākt P1 Incidenta risināšanu, bet citu darbu veikšanai nepieciešams iepriekšējs pircēja kontaktpersonas apstiprinājums. Par darbiem, kas ietilpst Platformas funkcijās, papildu maksu nepiemēro.

8. Plānotā apkope, attālinātā piekļuve un MDM

8.1. Datakom informē pircēja kontaktpersonu par plānoto apkopi vismaz 24 stundas iepriekš, izņemot gadījumus, kad drošības apstākļi prasa nekavējošu rīcību.

8.2. Ja pircējs 24 stundu laikā pēc paziņojuma saņemšanas neiesniedz pamatotus iebildumus vai nepiedāvā citu apkopes laiku, plānotā apkope uzskatāma par saskaņotu, izņemot 9.5. punktā minētās būtiskās izmaiņas, kurām nepieciešams nepārprotams apstiprinājums.

8.3. Ja pircējs noraida plānoto apkopi vai lūdz to pārcelt, Puses vienojas par citu laiku. Traucējumi vai Drošības incidenti, kas līdz apkopes veikšanai tieši izriet no tās neveikšanas, nav Datakom pienākumu pārkāpums.

8.4. Plānotās apkopes laiku neieskaita SLA termiņos.

8.5. Atjauninājumus un drošības labojumus lietotāju galiekārtās Datakom uzstāda automātiski bez iepriekšēja paziņojuma, un šīm darbībām 8.1. punktu nepiemēro. Ja nepieciešama ierīces restartēšana, lietotājs saņem paziņojumu. Serveru atjauninājumus Datakom uzstāda tikai ar pircēju iepriekš saskaņotā apkopes laikā.

8.6. Datakom uzstāda RMM aģentu katrā Pārvaldības apjomā iekļautajā iekārtā, kurā RMM aģenta uzstādīšana ir tehniski iespējama un ražotāja atbalstīta, vai nodod to pircējam uzstādīšanai. Piekrītot Noteikumiem, pircējs pilnvaro Datakom Abonementa termiņā uzstādīt, konfigurēt, atjaunināt un uzturēt RMM aģentus.

8.7. Izmantojot RMM aģentu, Datakom uzrauga iekārtu tehniskos rādītājus un notikumu žurnālus, attālināti pārvalda un konfigurē iekārtas, automātiski uzstāda drošības labojumus, integrē drošības rīkus un apkopo SLA mērīšanai un pārskatu sagatavošanai nepieciešamos datus.

8.8. RMM nereģistrē lietotāju taustiņsitienus, neveic nepārtrauktu lietotāju darbību novērošanu un neveido ekrāna ierakstus ārpus aktīvas attālinātās sesijas.

8.9. Datakom speciālists interaktīvu attālinātās piekļuves sesiju sāk, ja tam ir pircēja kontaktpersonas piekrišana vai sesija nepieciešama reģistrēta Pieteikuma risināšanai. Pirms sesijas sākuma Datakom informē pircēju. Automatizētām darbībām, piemēram, drošības labojumu uzstādīšanai vai iepriekš apstiprinātu skriptu izpildei, atsevišķa informēšana nav nepieciešama.

8.10. Pircējs var pārtraukt attālināto sesiju. Ja tas kavē Pieteikuma risināšanu, kavējuma laiku SLA termiņos neieskaita.

8.11. Izmantojot RMM, Datakom piemēro uz lomām balstītu piekļuves kontroli (RBAC), daudzfaktoru autentifikāciju administratīvajai piekļuvei un reģistrē attālinātās piekļuves sesijas, lai nodrošinātu to pārbaudāmību.

8.12. Pircējs bez Datakom rakstveida piekrišanas neatinstalē RMM aģentus un nemaina to konfigurāciju, izņemot darbības, kas objektīvi nepieciešamas Drošības incidenta ierobežošanai vai novēršanai. Pircējs iekļauj Datakom paziņotos RMM domēnus un IP adreses atļauto sarakstos un savlaicīgi informē Datakom par izmaiņām, kas var ietekmēt RMM darbību.

8.13. Mobilo ierīču pārvaldībai Datakom izmanto Microsoft Intune vai citu MDM risinājumu, par kuru Puses vienojas. Ierīci attālināti bloķē vai tās datus dzēš tikai pēc pircēja pieprasījuma vai saskaņā ar pircēja iepriekš apstiprinātu politiku. Datakom neatbild par datu zudumu, kas radies, pienācīgi izpildot šādu pircēja norādījumu vai apstiprinātu politiku, ja Datakom ir ievērojis attiecīgajai darbībai noteiktās prasības. Ja MDM risinājumā tiek reģistrēta darbinieka privātā ierīce, pircējs nodrošina tiesisko pamatu tās pārvaldībai un informē lietotāju par darbībām, ko pārvaldībā var veikt ar šo ierīci.

9. Izmaiņu un problēmu pārvaldība

9.1. Izmaiņa ir plānota darbība, kas ārpus Incidenta risināšanas maina IT infrastruktūras konfigurāciju, programmatūru, piekļuves tiesības vai drošības iestatījumus.

9.2. Standarta izmaiņa ir iepriekš noteikta, atkārtojama un zema riska darbība, piemēram, paroles atiestatīšana, lietotāja konta pievienošana vai standarta programmatūras instalēšana. Standarta izmaiņām atsevišķs apstiprinājums nav nepieciešams, ja tās veic iepriekš saskaņotajā kārtībā.

9.3. Normāla izmaiņa ir izmaiņa, kurai nepieciešama plānošana, riska novērtēšana un pircēja kontaktpersonas apstiprinājums 9.5. punktā noteiktajā kārtībā. Datakom pieteikumu sistēmā iesniedz izmaiņu pieprasījumu, norādot tās aprakstu, iespējamo ietekmi un atcelšanas plānu. Nebūtisku normālu izmaiņu Datakom drīkst veikt pēc pircēja kontaktpersonas apstiprinājuma vai, ja pircējs nav iebildis, 24 stundas pēc pieprasījuma saņemšanas (9.5. punkts).

9.4. Ārkārtas izmaiņa ir izmaiņa, kas nekavējoties nepieciešama Drošības incidenta ierobežošanai vai novēršanai vai kritiskas funkcijas atjaunošanai. Datakom drīkst sākt ārkārtas izmaiņu pirms apstiprinājuma saņemšanas, nekavējoties informējot pircēja kontaktpersonu, un dokumentē to pieteikumu sistēmā 24 stundu laikā pēc izmaiņas veikšanas.

9.5. Ja pircējs 24 stundu laikā pēc normālas izmaiņas pieprasījuma saņemšanas nesniedz apstiprinājumu vai pamatotus iebildumus, izmaiņa uzskatāma par apstiprinātu tikai tad, ja tā nevar būtiski ietekmēt sistēmu pieejamību, datu integritāti, autentifikācijas mehānismus vai būtisku lietotāju daļu. Šādām būtiskām izmaiņām vienmēr nepieciešams nepārprotams pircēja kontaktpersonas apstiprinājums. Šo punktu nepiemēro drošības pasākumiem, kuriem piemēro 10.2. punktu. Pircēja apstiprinājuma gaidīšanas laiku SLA termiņos neieskaita.

9.6. Ja izmaiņa izraisa Incidentu, Datakom nekavējoties mazina tā ietekmi vai izmaiņu atceļ. Ārkārtas izmaiņai atcelšanas plānu, ja tas piemērojams, Datakom dokumentē 24 stundu laikā pēc izmaiņas veikšanas.

9.7. Pēc pircēja pieprasījuma Datakom piecu Darbdienu laikā iesniedz izmaiņu žurnālu par pieprasīto periodu.

9.8. Problēma ir pastāvīgs vai atkārtots kļūmes cēlonis Pārvaldības apjomā, kas izraisa vairākus Incidentus vai pastāvīgi ietekmē IT infrastruktūras darbību.

9.9. Datakom reģistrē problēmas pieteikumu, ja viens un tas pats Incidents atkārtojas vismaz trīs reizes 30 dienu laikā, P1 vai P2 Incidents liecina par iespējamu sistēmisku cēloni vai pircējs pamatoti pieprasa problēmas analīzi.

9.10. Datakom veic pamatcēloņa analīzi (Root Cause Analysis, RCA) un 10 Darbdienu laikā pēc problēmas pieteikuma reģistrēšanas iesniedz pircējam ziņojumu. Ja analīzei nepieciešams piesaistīt trešo personu, Puses var vienoties par citu termiņu.

9.11. Datakom uztur identificēto problēmu un zināmo risinājumu reģistru un izmanto to atkārtotu Incidentu risināšanā.

10. Drošības pasākumi un pircēja lēmumi

10.1. Ja Platformas rīki vai Datakom konstatē kritisku ievainojamību vai apdraudējumu un pircēja piekrišanas gaidīšana var radīt būtisku risku IT infrastruktūrai vai datiem, Datakom drīkst īstenot tehniski nepieciešamus un samērīgus aizsardzības pasākumus bez pircēja iepriekšējas piekrišanas. Šādus pasākumus Pārvaldības apjomā veic Platformas rīki automātiski vai Datakom speciālisti atbilstoši SLA pieejamības laikam. Piekrītot Noteikumiem, pircējs pilnvaro Datakom veikt šīs darbības. Datakom par veiktajiem pasākumiem nekavējoties informē pircēja kontaktpersonu.

10.2. Ja drošības pasākumu ir iespējams saskaņot iepriekš, Datakom lūdz pircēja piekrišanu un nosaka atbildes termiņu, kas nepārsniedz 24 stundas. Ja pircējs termiņā neatbild vai pasākumu noraida, Datakom to neievieš un reģistrē šo apstākli pieteikumu sistēmā. Datakom neatbild par sekām tiktāl, ciktāl tās tieši izriet no attiecīgā drošības pasākuma neieviešanas pircēja lēmuma vai bezdarbības dēļ. SLA nepiemēro tikai šādi radītam kavējumam vai traucējumam.

10.3. Pircēja lēmums neieviest Datakom ieteikumu neierobežo Datakom tiesības ieteikumu atkārtot un pamatoti precizēt Pieteikuma prioritāti.

11. Trešo personu komponentes un intelektuālais īpašums

11.1. Datakom Platformā izmanto Trešo personu komponentes, ievērojot to licences noteikumus. Produktos iekļautās Trešo personu komponentes un to ražotāji ir norādīti Aprakstā.

11.2. Ja Trešo personu komponentes licences noteikumi ir tieši piemērojami pircējam, pircējs tos ievēro. Datakom pēc pircēja pieprasījuma sniedz savā rīcībā esošo informāciju par šiem noteikumiem.

11.3. Datakom pārvalda un uzrauga Platformā izmantotās Trešo personu komponentes. Trešās personas izraisīts darbības pārtraukums, ražotāja drošības labojumu pieejamības kavējums vai tādas komponentes funkciju vai licences izmaiņas, ko Datakom objektīvi nevar ietekmēt, paši par sevi nav Datakom pienākumu pārkāpums. Datakom veic saprātīgus pasākumus šo apstākļu ietekmes mazināšanai.

11.4. Aprakstā un Preces kartītē norādītu Trešo personu komponenti vai tās ražotāju Datakom maina tikai VV noteiktajā kārtībā. Noslēgtā Darījumā šādu maiņu veic ar pircēja piekrišanu. Iekšējos rīkus, kas Aprakstā nav norādīti, Datakom var mainīt, nesamazinot Platformas funkcijas.

11.5. Intelektuālā īpašuma tiesības uz Datakom programmatūru, skriptiem, automatizācijas risinājumiem, konfigurāciju veidnēm, metodēm, Platformas dokumentāciju, zinātību un RMM konfigurācijām pieder Datakom vai attiecīgajai trešajai personai. Pircējs saglabā tiesības uz savas IT infrastruktūras tehnisko dokumentāciju.

11.6. Pircējs saglabā tiesības uz saviem datiem un dokumentiem. Datakom tos apstrādā tikai Darījuma izpildei un saskaņā ar Noteikumu 13. nodaļu, ja tajos ir personas dati.

11.7. Pircējs nekopē, nedekompilē, neveic reverso inženieriju, neizplata, nesublicencē un nedara pieejamus trešajām personām Platformas aizsargātos elementus, izņemot normatīvajos aktos obligāti pieļautos gadījumus.

11.8. Datakom apliecina, ka tam ir tiesības nodrošināt Platformu un piešķirt pircējam 3.10. punktā noteiktās tiesības, un veic saprātīgus pasākumus, lai Platformas daļā, ko kontrolē Datakom, netiktu ieviesta ļaunprogrammatūra.

12. Pienākumu robežas un atbildība

12.1. Zaudējumu atlīdzības pamatu regulē VV 2. pielikuma 3.4. punkts. Šī nodaļa precizē Datakom pienākumu robežas un atbildības apmēru tiktāl, ciktāl tas nav pretrunā VV un piemērojamajiem normatīvajiem aktiem.

12.2. Datakom kiberdrošības pienākumu saturs un apjoms izriet no Noteikumu 4. un 10. nodaļas. Drošības incidenta iestāšanās pati par sevi nav Datakom pienākumu pārkāpums. Datakom rīcības atbilstību vērtē, ņemot vērā tā konkrētos pienākumus, VV un piemērojamos normatīvos aktus.

12.3. Traucējuma, datu zuduma vai Drošības incidenta sekas nav attiecināmas uz Datakom tiktāl, ciktāl tās tieši izraisījis vai palielinājis kāds no turpmāk minētajiem apstākļiem un Datakom ir pienācīgi izpildījis savus pienākumus:

- pircēja, tā lietotāju vai pircēja piesaistītu trešo personu darbība vai bezdarbība
- pircēja lietotāju rīcība pikšķerēšanas vai sociālās inženierijas uzbrukuma rezultātā, tostarp piekļuves datu izpaušana
- neprecīza vai nepilnīga pircēja sniegtā informācija vai nenodrošināta piekļuve
- ar Datakom nesaskaņota konfigurācijas maiņa
- pircēja noraidīts drošības pasākums vai apkope (8.3. un 10.2. punkts)
- neatbalstīta tehnoloģija (6.3. punkts) vai licenču trūkums (6.6.7. punkts)
- ārējs sakaru vai elektroapgādes traucējums
- ievainojamība vai uzbrukums, ko ar profesionālu rūpību un tajā brīdī pieejamiem tehniskajiem līdzekļiem nebija iespējams atklāt vai novērst

12.4. Platforma negarantē, ka IT infrastruktūra darbosies bez kļūdām, pārtraukumiem vai ievainojamībām vai ka tiks atklāts ikviens Drošības incidents.

12.5. Drošības incidenta gadījumā Datakom veic Noteikumos paredzētās incidenta konstatēšanas, sākotnējās reaģēšanas, ierobežošanas un novēršanas darbības Platformas funkciju un Pārvaldības apjoma robežās. Platformas funkcijās neietilpst padziļināta digitālā izmeklēšana, datu atjaunošana no rezerves kopijām vai IT infrastruktūras pilnīga atkārtota izveide pēc būtiska darbības pārtraukuma, ja vien Puses par šiem darbiem nav vienojušās atsevišķi. Paziņojumus kompetentajām iestādēm un datu subjektiem sniedz pircējs, savukārt Datakom tam palīdz 13.14. punktā noteiktajā apjomā.

12.6. Lēmumu par izpirkuma maksas maksāšanu pieņem pircējs. Datakom šādā maksājumā nepiedalās.

12.7. Pircējs veic saprātīgus pasākumus zaudējumu novēršanai un mazināšanai, saglabā pierādījumus un nodrošina Datakom iespēju izvērtēt prasījuma pamatā esošos apstākļus.

12.8. Datakom kopējais atbildības apmērs par visiem prasījumiem, kas izriet no viena Darījuma vai ir ar to saistīti, nepārsniedz 500 000 EUR (pieci simti tūkstoši euro) vai attiecīgā Darījuma cenu par 12 mēnešiem bez pievienotās vērtības nodokļa, ja šī cena pārsniedz 500 000 EUR. Šo ierobežojumu piemēro, ievērojot 12.9. punktu, VV un piemērojamos normatīvos aktus.

12.9. Atbildības ierobežojumu nepiemēro zaudējumiem, kas radušies Datakom apzinātas rīcības, rupjas neuzmanības vai ļauna nolūka dēļ, VV paredzētajiem līgumsodiem, kā arī gadījumos, kad atbildības ierobežošanu nepieļauj normatīvie akti.

12.10. Pircējs par iespējamu prasījumu rakstveidā informē Datakom 30 dienu laikā pēc tam, kad tas ir uzzinājis par prasījuma pamatā esošajiem apstākļiem. Paziņojuma kavējums neliedz celt prasījumu, bet tiek ņemts vērā, nosakot zaudējumu apmēru, ciktāl tas ierobežojis iespēju zaudējumus mazināt.

13. Personas datu apstrāde

13.1. Ciktāl Datakom, nodrošinot Platformas funkcijas, apstrādā personas datus pircēja vārdā, pircējs ir pārzinis un Datakom ir apstrādātājs Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (Vispārīgā datu aizsardzības regula, turpmāk - VDAR) 28. panta izpratnē. Šī nodaļa nosaka Pušu personas datu apstrādes noteikumus.

13.2. Ja pircējs pirkuma pieprasījumam pievieno savu apstrādes līgumu (VV 2. pielikuma 8.3. punkts), piemēro pircēja līgumu. Šādā gadījumā šo nodaļu piemēro tiktāl, ciktāl pircēja līgums attiecīgo jautājumu neregulē.

13.3. Apstrādes priekšmets un nolūks ir Platformas funkciju nodrošināšana. Apstrāde ietver personas datu saņemšanu, pārsūtīšanu, glabāšanu, strukturēšanu, attālinātu tehnisku apstrādi, uzraudzību, problēmu diagnostiku, drošības notikumu un Pieteikumu apstrādi, lietotāju un piekļuves administrēšanu, RMM darbību, rezerves kopēšanas statusa uzraudzību un pārskatu sagatavošanu.

13.4. Personas datu apstrāde ilgst Abonementa termiņu un pēc tā beigām tikai tik ilgi, cik nepieciešams 15. nodaļā paredzētajām darbībām pēc Abonementa beigām, datu atdošanai vai dzēšanai un tiesību aktos noteikto glabāšanas pienākumu izpildei.

13.5. Datu subjekti var būt pircēja darbinieki, amatpersonas, ārpakalpojumu sniedzēji, informācijas sistēmu lietotāji, klienti, sadarbības partneri un citas personas, kuru dati atrodas Pārvaldības apjomā iekļautajās sistēmās vai nonāk Pieteikumos, žurnālos vai drošības notikumos.

13.6. Personas datu kategorijas var būt identifikācijas un kontaktinformācija, lietotāju un kontu dati, ierīču un tīkla identifikatori, IP adreses, autentifikācijas un piekļuves metadati, darbību un tehniskie žurnāli, Pieteikumu un Drošības incidentu dati un saziņas metadati.

13.7. Par pircēja dokumentētiem norādījumiem uzskatāmi Noteikumi, pirkuma pasūtījums, pircēja apstiprinātā Platformas konfigurācija un pieteikumu sistēmā vai citā rakstveida formā sniegti pircēja kontaktpersonu norādījumi, ciktāl tie ir tiesiski, attiecas uz Darījuma izpildi un ir tehniski izpildāmi.

13.8. Platformas standarta konfigurācija nav paredzēta īpašu kategoriju personas datu vai personas datu par sodāmību un pārkāpumiem mērķtiecīgai apstrādei. Ja šādi dati atrodas Pārvaldības apjomā un to apstrāde ir objektīvi nepieciešama, pircējs nodrošina atbilstošu tiesisko pamatu un informē Datakom par nepieciešamajiem drošības pasākumiem.

13.9. Datakom apstrādā personas datus tikai saskaņā ar pircēja dokumentētiem norādījumiem, izņemot gadījumus, kad datu apstrādi pieprasa Datakom piemērojami Eiropas Savienības vai dalībvalsts tiesību akti. Šādā gadījumā Datakom pirms apstrādes informē pircēju, ja vien tiesību akti to neaizliedz. Datakom nodrošina, ka personas datiem piekļūst tikai pienācīgi pilnvarotas personas, kurām ir konfidencialitātes pienākums. Ja Datakom uzskata, ka pircēja norādījums pārkāpj VDAR vai citus piemērojamos personas datu aizsardzības noteikumus, Datakom par to nekavējoties informē pircēju.

13.10. Pircējs piešķir Datakom vispārēju rakstisku atļauju piesaistīt apakšapstrādātājus, kuri norādīti Aprakstā. Pirms jauna apakšapstrādātāja piesaistīšanas vai esošā nomaiņas Datakom vismaz 15 Darbdienas iepriekš rakstveidā informē pircēju par paredzētajām izmaiņām un dod iespēju šajā termiņā pamatoti iebilst. Ja pircējs iebilst, Puses izvērtē alternatīvu risinājumu. Līdz iebilduma atrisināšanai attiecīgo jauno apakšapstrādātāju pircēja datu apstrādē neiesaista. Datakom ar katru apakšapstrādātāju noslēdz saistošu vienošanos, uzliekot tam pēc būtības līdzvērtīgus datu aizsardzības pienākumus, un atbild par šo pienākumu izpildi VDAR 28. panta 4. punktā noteiktajā kārtībā. Ja apakšapstrādātājs vienlaikus ir apakšuzņēmējs VV izpratnē, tā piesaistīšanu vai nomaiņu veic arī VV noteiktajā kārtībā.

13.11. Personas datu apstrādes, tostarp datu glabāšanas, vietas un apakšapstrādātāji norādīti Aprakstā. Datu glabāšanas vieta un attālinātās piekļuves vai citas datu apstrādes vieta var atšķirties. Ja personas dati tiek nodoti ārpus Eiropas Ekonomikas zonas, Datakom nodrošina VDAR V nodaļai atbilstošu nodošanas pamatu un ievēro pircēja dokumentētos norādījumus. Pircējs pirkuma pieprasījuma komentārā var norādīt datu glabāšanas teritorijas ierobežojumu (VV 3. pielikuma 1.4.5. punkts), kas pats par sevi nav uzskatāms par aizliegumu veikt jebkādu attālinātu piekļuvi no citas teritorijas. Šādus ierobežojumus Puses precizē Darījumā.

13.12. Datakom īsteno personas datu apstrādes riskam atbilstošus tehniskos un organizatoriskos drošības pasākumus, tostarp piekļuves tiesību pārvaldību, daudzfaktoru autentifikāciju administratīvajai piekļuvei, audita žurnālu uzturēšanu, ievainojamību pārvaldību un šifrēšanu atbilstoši apstrādes raksturam.

13.13. Datakom bez nepamatotas kavēšanās pēc personas datu aizsardzības pārkāpuma konstatēšanas informē pircēju, ja pārkāpums skar pircēja vārdā apstrādātos datus. Datakom sniedz tā rīcībā esošo informāciju par pārkāpumu, tā iespējamām sekām un veiktajiem pasākumiem. Papildu informāciju Datakom sniedz, tiklīdz tā kļūst pieejama.

13.14. Datakom, ņemot vērā apstrādes raksturu un tā rīcībā esošo informāciju, samērīgā apjomā palīdz pircējam izpildīt pienākumus attiecībā uz datu subjektu pieprasījumiem, apstrādes drošību, personas datu aizsardzības pārkāpumu paziņošanu, ietekmes uz datu aizsardzību novērtējumiem un iepriekšēju apspriešanos ar uzraudzības iestādi.

13.15. Datakom dara pircējam pieejamu informāciju, kas nepieciešama VDAR 28. pantā noteikto pienākumu izpildes apliecināšanai, un ļauj pircējam vai tā pilnvarotam auditoram veikt atbilstības pārbaudes, tostarp

auditus, un tajos sadarbojas. Puses vispirms izmanto pieejamos sertifikātus, neatkarīgu auditu ziņojumus un citus samērīgus pierādījumus. Pircējs par plānotu auditu parasti paziņo vismaz 20 Darbdienas iepriekš. Auditus parasti veic ne biežāk kā reizi 12 mēnešos, ja vien pamatotas aizdomas par pārkāpumu, nozīmīgs Drošības incidents, uzraudzības iestādes prasība vai tiesību akti neattaisno ārpuskārtas pārbaudi. Auditu organizē, ievērojot citu klientu datu konfidencialitāti un Platformas drošību.

13.16. Pēc Abonementa beigām Datakom pēc pircēja izvēles atdod pircējam vai dzēš personas datus, kas apstrādāti pircēja vārdā, un dzēš esošās datu kopijas, izņemot gadījumus, kad glabāšanu pieprasa Eiropas Savienības vai dalībvalsts tiesību akti. Datakom pirms Abonementa beigām informē pircēju par datu atdošanas un dzēšanas tehnisko kārtību, tostarp par rezerves kopiju dzēšanas ciklu. Kamēr datu kopijas tehnisku iemeslu dēļ vēl nav dzēstas, Datakom tās izolē no ikdienas apstrādes, nodrošina to aizsardzību un dzēš saskaņā ar dokumentētu grafiku, nepieļaujot izmantošanu jauniem nolūkiem.

14. Konfidencialitāte

14.1. Konfidenciāla informācija ir informācija, ko viena Puse nodod otrai un ko pēc tās rakstura vai norādes var saprātīgi uzskatīt par konfidenciālu, tostarp IT infrastruktūras un Platformas arhitektūra, konfigurācijas, drošības informācija, Pieteikumu un Incidentu dati, ievainojamības un tehniskā dokumentācija.

14.2. Puse, kas saņēmusi Konfidenciālu informāciju, izmanto to tikai Darījuma izpildei un aizsargā vismaz ar tādu pašu rūpību, kādu tā piemēro savai līdzvērtīgai konfidenciālai informācijai.

14.3. Puse drīkst izpaust Konfidenciālu informāciju saviem darbiniekiem, apakšuzņēmējiem un konsultantiem tikai tad un tādā apjomā, kādā informācija tiem nepieciešama Darījuma izpildei un uz tiem attiecas konfidencialitātes pienākums.

14.4. Konfidencialitātes pienākums neattiecas uz informāciju, kas ir publiski pieejama bez Noteikumu pārkāpuma, likumīgi saņemta no trešās personas bez konfidencialitātes ierobežojuma vai neatkarīgi izstrādāta, kā arī uz informāciju, kuras izpaušanu pieprasa normatīvais akts, tiesa vai kompetenta iestāde. Darījuma cena un VV nav Konfidenciāla informācija. Noteikumi neierobežo pircēja pienākumus saskaņā ar Informācijas atklātības likumu.

14.5. Ja Konfidenciāla informācija jāizpauž obligāti, Puse, ciktāl to pieļauj normatīvie akti, iepriekš informē otru Pusi un izpauž tikai obligāti nepieciešamo informāciju.

14.6. Konfidencialitātes pienākums ir spēkā piecus gadus pēc Abonementa beigām, bet attiecībā uz komercnoslēpumu un personas datiem tik ilgi, kamēr pastāv to aizsardzības pamats.

15. Abonementa beigas

15.1. Pēc Abonementa beigām pircējs pārtrauc lietot Platformas programmatūru un Datakom piekļuves līdzekļus, izņemot 15.2. punktā paredzētās nodošanas darbības.

15.2. Datakom 30 dienu laikā pēc Abonementa beigām nodod pircējam pircēja IT infrastruktūras tehnisko dokumentāciju (4.2.2. punkts) un piekļuves informāciju, deaktivizē RMM aģentus un, ciktāl tas tehniski iespējams, attālināti tos noņem no pircēja iekārtām. Puses savlaicīgi saskaņo nodošanai nepieciešamo ierobežoto piekļuvi un tās pārtraukšanas secību. Pircējs nodrošina iekārtu pieejamību nodošanas darbībām un pēc to pabeigšanas nekavējoties bloķē Datakom lietotāju kontus un nomaina attiecīgās paroles. Drošības apsvērumu dēļ pircējs drīkst piekļuvi atsaukt arī agrāk, par to informējot Datakom un vienojoties par citu drošu nodošanas veidu.

15.3. Personas datu atdošanu vai dzēšanu Datakom veic saskaņā ar 13.16. punktu.

15.4. Noteikumi par konfidencialitāti, personas datiem un intelektuālo īpašumu ir spēkā arī pēc Abonementa beigām.

16. Saziņa

16.1. Ikdienas jautājumos par Platformas darbību, Pieteikumiem, plānotajiem darbiem un citiem tehniskiem jautājumiem Puses sazinās pa e-pastu, pieteikumu sistēmā vai klientu portālā.

16.2. Paziņojumus par Darījuma izbeigšanu, būtiskiem pārkāpumiem, prasījumiem un citiem juridiski nozīmīgiem jautājumiem Puses sniedz VV noteiktajā kārtībā.

16.3. Puses bez nepamatotas kavēšanās informē viena otru par kontaktpersonu un saziņas rekvizītu izmaiņām. Līdz atbilstoša paziņojuma saņemšanai Datakom izmanto pēdējo pircēja norādīto kontaktinformāciju.

16.4. Informatīvus paziņojumus par atjauninājumiem, drošības labojumiem, plānotajiem darbiem vai Incidentiem Datakom var nosūtīt elektroniski vai publicēt pieteikumu sistēmā.

17. Noslēguma noteikumi

17.1. Datakom Darījuma izpildē var iesaistīt apakšuzņēmējus VV noteiktajā kārtībā. Datakom atbild par saviem pienākumiem arī tad, ja tos izpilda apakšuzņēmējs.

17.2. Puses ievēro tām piemērojamās starptautiskās sankcijas un eksporta un importa kontroles prasības. Datakom ir tiesīgs atteikt vai apturēt tādas Platformas komponentes piegādi, kuras nodrošināšana pārkāptu Datakom piemērojamās tiesību normas.

17.3. Ja kāds Noteikumu punkts kļūst spēkā neesošs vai nav piemērojams, tas neietekmē pārējo Noteikumu spēkā esību.

17.4. Noteikumiem piemēro Latvijas Republikas normatīvos aktus. Strīdus Puses risina VV noteiktajā kārtībā.

Pielikums. Datakom un pircēja pienākumu sadalījums

Tabula apkopo Noteikumos noteikto pienākumu sadalījumu. Ja tabula atšķiras no Noteikumu punkta, piemēro Noteikumu punktu.

Joma	Datakom	Pircējs
Piekļuve un informācija	Izmanto piekļuvi tikai Platformas funkciju nodrošināšanai. Piemēro RBAC, MFA un attālinātās piekļuves sesiju reģistrēšanu. Pēc Abonementa beigām nodod dokumentāciju un piekļuves informāciju 15.2. punktā noteiktajā kārtībā.	Nodrošina piekļuvi, informāciju un kontaktpersonas (6.1. un 6.2. punkts). Pēc nodošanas darbību pabeigšanas bloķē Datakom kontus un nomaina paroles (15.2. punkts).
Licences	Nodrošina Produktā iekļautās Trešo personu komponentes. Norāda pircējam nepieciešamās licences pirms funkcijas ieviešanas.	Nodrošina Microsoft licences ar Intune Plan 1 un Entra ID P1 funkcijām, citas nepieciešamās licences, maksas Knox Suite licences un pārējās 6.6. punktā minētās licences.
Programmatūras versijas	Informē par neatbalstītām tehnoloģijām.	Lieto ražotāju atbalstītas versijas (6.3. punkts).
RMM	Uzstāda, konfigurē, atjaunina un uztur RMM aģentus.	Neatinstalē RMM aģentus un nemaina to konfigurāciju bez saskaņošanas, izņemot Drošības incidenta ierobežošanai nepieciešamo. Iekļauj Datakom paziņotās adreses atļauto sarakstos.
Galiekārtu aizsardzība (AV, EDR)	Pārvalda, uzrauga un atjaunina AV un EDR risinājumus Pārvaldības apjomā (4.3.2. punkts).	Nodrošina Datakom piekļuvi un informē par izmaiņām, kas var ietekmēt AV un EDR darbību (6.2. un 6.4. punkts).
Mobilās ierīces (MDM)	Pārvalda MDM reģistrētās ierīces un apstiprinātās politikas. Ierīci bloķē vai tās datus dzēš pēc pircēja pieprasījuma vai apstiprinātas politikas (8.13. punkts).	Nodod ierīces pārvaldībā, apstiprina politikas, nekavējoties ziņo par nozaudētām ierīcēm, nodrošina tiesisko pamatu privātu ierīču pārvaldībai (6.4. un 8.13. punkts).
Atjauninājumi un ielāpi	Izvērtē un uzstāda atjauninājumus, ja tie pieejami un tehniski piemērojami, ievērojot 4.3.6. un 8.5. punktu.	Nodrošina piekļuvi iekārtām un informāciju, kas nepieciešama atjauninājumu uzstādīšanai (6.2. punkts).
Daudzfaktoru autentifikācija (MFA)	Konfigurē un pārvalda Pārvaldības apjomā.	Nodrošina lietotāju sadarbību saskaņoto identitātes drošības politiku īstenošanā (6.2. un 4.5. punkts).
Paroles politika	Konfigurē un uzrauga.	Nodrošina informāciju un piekļuvi paroles politikas piemērošanai (6.2. un 4.5. punkts).
E-pasta drošība	Konfigurē un uzrauga filtrus un politikas.	Informē Datakom par izmaiņām, kas var ietekmēt e-pasta aizsardzību (6.4. punkts).
Drošības apmācība	Nodrošina pikšķerēšanas simulācijas un tiešsaistes apmācību moduļus, ja Produktā ietilpst Nimblr. Sniedz ieteikumus.	Organizē klātienes apmācības un lietotāju informēšanu.
Rezerves kopēšana	Uzrauga rezerves kopēšanas uzdevumu statusu un Platformas rīku iespēju robežās novērš ar uzdevumu izpildi saistītās kļūdas (4.4. punkts).	Nodrošina rezerves kopēšanas risinājumu, nosaka kritiskos datus, RPO un RTO. Atbild par rezerves kopiju esību un datu atjaunošanas organizēšanu.
Tīkla drošība	Atjaunina norādīto tīkla iekārtu programmaparatūru, veido konfigurāciju rezerves kopijas un uztur uzskaiti (4.6. punkts).	Tīkla iekārtu konfigurāciju un piekļuves noteikumus maina tikai pēc saskaņošanas ar Datakom (6.4. punkts).
Fiziskā drošība	Neuzņemas IT infrastruktūras fiziskās drošības pienākumus.	Nodrošina telpu piekļuves kontroli un iekārtu fizisko aizsardzību.
Incidentu reaģēšana	Veic sākotnējo reaģēšanu, ierobežošanu un Incidentu risināšanu Platformas funkciju un Pārvaldības apjoma robežās. Papildu izmeklēšana un pilnīga sistēmu atkārtota izveide nav iekļautas (12.5. punkts).	Sadarbojas, pieņem lēmumus par jautājumiem, kas ietekmē pircēja darbības procesus, sniedz paziņojumus iestādēm un datu subjektiem un lemj par izpirkuma maksu.
Audits un normatīvā atbilstība	Sniedz Platformā pieejamo informāciju un atbalstu.	Nosaka savus normatīvos pienākumus, ierosina auditus un izpilda šos pienākumus.