**Tehniskā specifikācija**

**Rīgas satiksmes pasažiera lietotnes attīstība**

**Iepirkuma priekšmets:** Rīgas satiksmes pasažiera mobilās lietotnes (turpmāk – Lietotne) drošības un pieejamības uzlabojumi, funkcionalitātes paplašināšana un pielāgošana atjauninātajai Digitālo biļešu sistēmai.

1. **Esošās situācijas apraksts:**
	1. Lietotne nodrošina Rīgas sabiedriskā transporta pasažieriem iespēju tiešsaistē:
		1. iegādāties koda biļetes, samaksājot par pirkumu ar bankas karti;
		2. reģistrēt braucienu, iekāpjot sabiedriskajā transportlīdzeklī un noskenējot kvadrātkodu vai ievadot to manuāli;
		3. uzrādīt reģistrēto biļeti kontrolei;
		4. apskatīt darījumu un braucienu vēsturi.
	2. Lietotnes lietotāju reģistrācija, koda biļešu veidu izgūšana, transakciju reģistrēšana, biļešu saņemšana pēc veiksmīgas apmaksas un braucienu reģistrācija notiek, izmantojot Digitālo biļešu sistēmas piekļuves programmsaskarnes metodes.
	3. Lietotne pieejama lejupielādei elektroniskajos veikalos Google Play: [Rīgas satiksmes koda biļete — Lietotnes pakalpojumā Google Play](https://play.google.com/store/apps/details?id=com.flutter.rspassenger&hl=lv&gl=US) un App Store: [Rīgas satiksmes koda biļete on the App Store (apple.com)](https://apps.apple.com/us/app/r%C4%ABgas-satiksmes-koda-bi%C4%BCete/id1584070455).
2. **Lietotnes komponentes:**
	1. Lietotnes Android un iOS versija;
	2. Lietotnes aizmugursistēmas datubāze, pārvaldības panelis un piekļuves programmsaskarnes (turpmāk – API) metodes (turpmāk viss kopā – RSPS);
	3. RSPS produkcijas, testa un izstrādes vides infrastruktūra – Kubernetes klasteri (Azure Kubernetes service) 3 gab., PostgreSQL DB (Azure PostgreSQL flexible server) 3 gab.;
	4. programmatūras piegāžu vide – GitLab/Git SaaS RSPS zaros un Azure konteineru reģistrs.
3. **ITIL ITSM (Support level) vadlīnijas**
	1. Avārija – problēma, kas izraisa pilnīgu RSPS apstāšanos un/vai funkciju nepieejamību (**1.kategorija - uzturēšana**).
	2. Kļūda, ko nevar apiet – problēma, ko izraisījusi RSPS programmatūras kļūda, vai nekorekta darbība un kas rada ievērojamus funkcionalitātes zudumus un nav zināms problēmas apiešanas risinājums, bet ir iespējams darbu turpināt ierobežotā režīmā (**2.kategorija - garantija**).
	3. Kļūda, ko var apiet – problēma, kas izraisa minimālus iespēju un/vai funkciju zudumus, ietekme uz RSPS ir mazsvarīga vai sagādā neērtības (**3.kategorija - garantija**).
	4. Neprecizitāte – problēma, kas neizraisa iespējamus zudumus un ir uzskatāma par RSPS programmatūras kļūdu, neprecizitāti vai nekorektu darbību, kas rada nelielu ietekmi uz darbu RSPS (**4.kategorija - garantija**).
	5. Izmaiņas – pieprasījums veikt izmaiņas vai papildināt RSPS funkcionalitāti, dokumentāciju, vai veikt citus papildu darbus, kas atšķiras no iepriekš aprakstītajām kategorijām (**6.kategorija – izmaiņu pieprasījums**).
4. **Lietotnes drošības un pieejamības uzlabojumi:**
	1. Reģistrēšanas process:
		1. Nodrošināt jaunu Lietotnes lietotāju reģistrēšanu ar e-pastu un paroli, sūtot uz norādīto e-pasta adresi apstiprināšanas saiti.
		2. Ļaut ar e-pastu reģistrētam Lietotnes lietotājam savā profilā papildus reģistrēt mobilā tālruņa numuru, sūtot uz to SMS īsziņu ar verifikācijas kodu.
		3. Visiem Lietotnes lietotāju reģistrētiem e-pastiem un tālruņu numuriem jābūt unikāliem.
		4. Ja Lietotnes lietotājs jau ir reģistrēts ar mobilā tālruņa numuru, ļaut viņam savā profilā papildus reģistrēt e-pastu, sūtot uz norādīto e-pasta adresi apstiprināšanas saiti.
		5. Nodrošināt Lietotnes lietotājam iespēju atjaunot paroli gan sūtot SMS īsziņu ar verifikācijas kodu uz profilā noradīto mobilā tālruņa numuru, gan sūtot apstiprināšanas saiti uz profilā norādīto e-pasta adresi.
		6. Nodrošināt automatizētu dinamisku lietotāja pārbaudi, veicot Lietotnes lietotāja reģistrāciju vai paroles atjaunošanu, lai pārliecinātos, ka lietotājs ir cilvēks, nevis mašīna.
		7. Regulāri automātiski atjaunot reģistrācijas / ielogošanās skata tālruņa numura ievadīšanas logā mobilo tālruņu valstu kodus.
	2. Koda biļešu pieejamība:
		1. Nodrošināt iespēju Lietotnes lietotājam pievienot savam Lietotnes kontam pie cita tirgotāja iegādāto koda biļeti, ja tirgotājam nav savas mobilās lietotnes un Lietotnes lietotājam pieejams iegādātās koda biļetes kvadrātkods drukātā vai digitālā attēla veidā.
		2. Nodrošināt iespēju Lietotnes lietotājam apskatīt un izmantot pie cita tirgotāja iegādātās koda biļetes, ja tirgotājam ir sava mobilā lietotne.
	3. Drošības un pieejamības risku mazināšana / novēršana:
		1. Novērst Lietotnes darbības kļūdu, kad, atverot Lietotni, lietotājam tiek rādīts sākumskats ar Pasūtītāja logo bez pogām, no kura nav iespējams pāriet pie nākamajiem skatiem un uzsākt Lietotnes lietošanu, vai Lietotnes atvēršanas procesā raustās sākumekrāns.
		2. Liegt Lietotnes lietotājam uzņemt Lietotnes pēdējā brauciena reģistrācijas skata ekrānuzņēmumu.
		3. Ieviest kontroles mehānismu un neļaut vienam un tam pašam lietotājam ielogoties Lietotnē no vairākām viedierīcēm vienlaicīgi.
		4. Papildināt RSPS pārvaldības paneli ar bankas karšu dzēšanas funkciju gadījumam, kad pie Pasūtītāja vēršas Lietotnes lietotājs – bankas kartes īpašnieks ar lūgumu dzēst viņam piederošo bankas karti no viņa un / vai citu lietotāju profiliem.
		5. Nodrošināt, saskaņojot ar Pasūtītāju, regulāru automātisku Lietotnes lietotāju dzēšanu, ja Digitālo biļešu sistēmā, kas emitē koda biļetes un reģistrē braucienus, tie ir dzēsti vai deaktivizēti.
		6. Izveidot programmatūras piegāžu vidē CI/CD pipeline, iekļaujot automatizētus koda kvalitātes un drošības pārbaudes.
		7. Veikt esošo API metožu auditu, sagatavot un izvietot to aprakstus GitLab repozitorijā atbilstoši faktiskajam pirmkodam, saglabājot tur esošo sadalījumu:
			1. private API,
			2. public API,
			3. report API,
			4. verification API.
		8. Izveidot kļūdu un atbilstošo kļūdas paziņojumu klasifikatoru 3 valodās – latviešu, angļu un ukraiņu valodā, kuru Pasūtītājs var patstāvīgi pārvaldīt, rediģēt tekstus, pievienot un dzēst kļūdu kodus.
		9. Nodrošināt IP adreses, iekārtas identifikatora un mobilās Lietotnes izstrādātāja versijas, no kuras tiek sūtīts pieprasījums Digitālo biļešu sistēmai, nodošanu saglabāšanai Digitālo biļešu sistēmā pie katras darbības.
		10. Nodrošināt lietotājam iespēju Lietotnē apskatīt pamatdatus par lietotāju, Lietotnes versiju u.tml., kas nepieciešams lietotāju atbalsta nodrošināšanai, datu apjomu un vizualizāciju saskaņojot ar Pasūtītāju.
5. **Lietotnes funkcionalitātes paplašināšana:**
	1. Integrēt Lietotnē Pasūtītāja rīcībā esošo virtuālo tablo (turpmāk – Tablo), kurā ir pieejami aktuālie Rīgas sabiedriskā transporta maršruti, maršrutu plānotājs, maršrutu karte, plānotie kustības saraksti un prognozētie sabiedrisko transportlīdzekļu (turpmāk – STL) pienākšanas laiki tiešsaistes režīmā, un kurš realizēts kā WEB lietotne.
	2. Nodrošināt Tablo saskarnes pieejamību 3 valodās – latviešu, angļu un ukraiņu valodā ar iespēju lietotājam izvēlēties sev vēlamo valodu. Tekstu tulkošanu, ja tāda ir nepieciešama, nodrošina Pasūtītājs.
	3. Ja Tablo nav pieejams vai viedtālrunī nav tīmekļa savienojuma, rādīt Lietotnes lietotājam attiecīgo paziņojumu, tekstu saskaņojot ar Pasūtītāju.
	4. Pārējo Lietotnes funkcionalitāti saglabāt nemainīgu.
6. **Izmaiņu pieprasījumi:**
	1. Sagatavot izmaiņu aprakstu, kas nepieciešams šīs Tehniskās specifikācijas 4. un 5. punktā noteikto Lietotnes drošības uzlabojumu un funkcionalitātes paplašināšanas realizācijai, to realizācijas un ieviešanas plānu (turpmāk – Izmaiņu plāns) un saskaņot to ar Pasūtītāju.
	2. Veikt izmaiņas saskaņā ar Izmaiņu plānu.
	3. Izmaiņu plānā papildus iekļaut citus Piegādātāja priekšlikumus Lietotnes attīstībai, piemēram, uzticamības (drošuma), veiktspējas efektivitātes, drošības, elastīguma un mērogojamības uzlabojumus.
	4. Sastādot Izmaiņu plānu, plānot piegādes Sprintos, katram nodevumam paredzot akcepttestēšanu, kas noteikta šīs tehniskās specifikācijas 7.2.-7.6. apakšpunktā, bet gala nodevumam papildus – Pasūtītāja nodrošinātā Lietotnes drošības auditu par atbilstību Latvijas Republikas Ministru kabineta 28.07.2015. noteikumiem Nr.442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”.
	5. Piegādātājs nodrošina izmaiņu pieprasījumu izpildi, atbilstoši un ievērojot ITIL ITSM (Support level) vadlīnijas ar specifiskām pieteikumu kategorijām un to prioritātēm. (6. kategorijas pieteikumi).
	6. Piegādātājs nodrošina realizācijas piedāvājuma sagatavošanu (darba uzdevuma) 6.kategorijas pieteikumiem bez maksas.
	7. Izmaiņu pieprasījuma darba uzdevums tiek saskaņots un apstiprināts ar Pasūtītāju.
	8. Plānotais izmaiņu un RSPS attīstības pieteikumu (6.kategorija) darbu apjoms ne vairāk kā 10% no līgumā noteiktās uzturēšanas maksas.
	9. Reakcijas laiks 6. kategorijas pieteikumam ir ne ilgāk kā 5 darbdienas, kura ietvarā sagatavo piedāvājumu, kas satur risinājuma aprakstu un darbietilpības novērtējumu. Ja piedāvājuma sagatavošanai Piegādātājs ir pieprasījis Pasūtītājam papildu informāciju, darbdienu skaitīšana tiek apturēta uz laiku, līdz Pasūtītājs ir iesniedzis Piegādātājam pieprasīto informāciju.
7. **Nefunkcionālās prasības:**
	1. Sagatavot Lietotnes dokumentāciju, tās saturu, dokumentu veidus, noformējumu un iesniegšanas kārtību, saskaņojot ar Pasūtītāju.
	2. Veikt Lietotnes pilna cikla testēšanu izstrādes vidē.
	3. Sagatavot un iesniegt Pasūtītājam programmatūras un konfigurēšanas nodevumu kopā ar instrukciju Pasūtītāja sistēmas administratoram par nodevuma ieviešanu Pasūtītāja testa vidē.
	4. Ja Pasūtītājs, veicot piegādātā nodevuma pārbaudi testa vidē, **konstatē** nepilnības vai trūkumus, novērst tos un atkārtoti izpildīt šīs tehniskās specifikācijas 7.2. un 7.3. apakšpunktu.
	5. Ja Pasūtītājs, veicot piegādātā nodevuma pārbaudi testa vidē, **nekonstatē** nepilnības vai trūkumus, sagatavot un iesniegt Pasūtītājam programmatūras un konfigurēšanas nodevumu kopā ar instrukciju Pasūtītāja sistēmas administratoram par nodevuma ieviešanu Pasūtītāja **produkcijas vidē**.
	6. Ja Pasūtītājs, veicot piegādātā nodevuma pārbaudi produkcijas vidē, **konstatē** nepilnības vai trūkumus, novērst tos un atkārtoti izpildīt šīs tehniskās specifikācijas 7.2.-7.5. apakšpunktu.
	7. Veicot risinājuma piegādi, Piegādātājs nodrošina tā izvietošanu Pasūtītāja testa vidē, kā arī veic izmaiņas Lietotnes dokumentācijā, ja tāda jau ir piegādāta saskaņā ar šīs Tehniskās specifikācijas 7.1. apakšpunktu.
	8. Pēc Pasūtītāja pieprasījuma sniegt atbalstu Lietotnes publicēšanā App Store un Google Play elektroniskajos veikalos (turpmāk – Elektroniskie veikali), kā arī sagatavot publicēšanai Elektroniskajos veikalos visus nepieciešamos ekrānskatus visos nepieciešamajos izmēros.
	9. Nodot Pasūtītājam visas autora mantiskās un izņēmuma tiesības uz visiem darbu rezultātā radītajiem un pilnā apmērā apmaksātajiem autortiesību objektiem.
	10. Lai nodrošinātu uzskaitīto darbu veikšanu, Pasūtītājs nodrošina:
		1. piekļuvi Lietotnes pirmkodam;
		2. piekļuvi Lietotnes aizmugursistēmas datubāzei, pārvaldības panelim un API metodēm;
		3. piekļuvi izstrādes videi;
		4. piekļuvi citiem resursiem un infrastruktūras objektiem, ja izstrādes laikā tiek konstatēta šāda nepieciešamība.

**8. Citas prasības:**

**8.1. Arhitektūra**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| Lietotnes komponentes | Lietotnē tiek izmantotas šādas komponentes:1. Lietotnes Android un iOS versija;
2. Lietotnes aizmugursistēmas datubāze, pārvaldības panelis un piekļuves programmsaskarnes metodes;
3. RSPS produkcijas, testa un izstrādes vides infrastruktūra – Kubernetes klasteri (Azure Kubernetes service) 3 gab., PostgreSQL DB (Azure PostgreSQL flexible server) 3 gab.;
4. programmatūras piegāžu vide – GitLab/Git SaaS RSPS zaros un Azure konteineru reģistrs.
 |
| RSPS vides | RSPS ir paredzētas šādas vides:1. **Produkcijas vide.** Produkcijas vidi nodrošina Pasūtītājs un tā paredzēta Lietotnes darbināšanai produkcijas režīmā;2. **Testa vide.** Testa vidi nodrošina Pasūtītājs, un tā paredzēta Lietotnes testēšanai, t.sk. akcepttestēšanai no Pasūtītāja puses, kā arī apmācībām;3. **Izstrādes vide.** Izstrādes vidi nodrošina Piegādātājs un tā ir paredzēta Lietotnes izstrādei un testēšanai no Piegādātāja puses.Visas izmaiņas Lietotnē un RSPS veicamas vispirms testa vidē un pēc saskaņošanas ar Pasūtītāju tiek izvietotas produkcijas vidē.Produkcijas un testa vides uzstādīšanu veic Pasūtītājs vai tā pārstāvis atbilstoši Piegādātāja dotajām instrukcijām un norādēm, un, ja nepieciešams – atbalstu.Piegādātājs sagatavo Lietotnes Android un iOS testa versiju pārbaudei pret Pasūtītāja testa vidi (skat. šīs tehniskās specifikācijas 7.4. apakšpunktu) un Android un iOS produkcijas versiju pārbaudei pret Pasūtītāja produkcijas vidi (skat. šīs tehniskās specifikācijas 7.6. apakšpunktu) un izplatīšanai, izmantojot Elektroniskos veikalus. |

**8.2. Pieejamība**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| Pieejamības rādītāji | Lietotnei ir jānodrošina nepārtraukta pieejamība lietotājiem 24 stundas diennaktī un 7 dienas nedēļā. Lietotnes darbspējas laikam jābūt ne mazākam kā 99,9% mēnesī, izņemot plānotās un ar Pasūtītāju saskaņotās dīkstāves. |
| Darbības nepārtrauktība | Programmatūras nodevumu uzstādīšanu jāveic bez vai ar minimāliem, ar Pasūtītāju saskaņotiem, Lietotnes darbības pārtraukumiem. |
| Programmkoda kvalitātes pārbaude | Programmatūras izstrādes laikā Piegādātājam ir jāveic programmkoda kvalitātes kontrole, jānodrošina preventīvās un korektīvās darbības. |

**8.3. Veiktspēja**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| RSPS un Lietotnes veiktspēja | RSPS jāvar apstrādāt 1000 vienlaicīgus lietotāju pieprasījumus, bez ietekmes uz pieprasījumu izpildes laiku. Atbildes laiks Lietotnē uz vienkāršiem pieprasījumiem nedrīkst pārsniegt 2 sekundes, bet vēsturiskās informācijas ielādes laiks nedrīkst pārsniegt 4 sekundes. |
| Veiktspējas pārbaude | Piegādātājam jāveic veiktspējas pārbaude testa vidē pirms Lietotnes palaišanas produkcijā (*pre-production*), kā arī jānodrošina veiktspējas testēšanas scenāriju izpildei nepieciešamo programnodrošinājumu un testa scenāriju saskaņošana. |
| RSPS monitorings | Lietotnei jānodrošina programmatūras kļūdu un izņēmumu paziņošanas funkcionalitāte, kā arī brīdinājumu nosūtīšana no RSPS par Lietotnes resursu nepietiekamību.Lietotnes un RSPS monitorings ir jāveic vismaz lietotāju saskarnes, Lietotnes un datubāzes līmenī. |

**8.4. Drošība**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| Lietotāju autentifikācija | RSPS jānodrošina lietotāju autentifikācija un autorizācija, izmantojot aktīvo direktoriju (AD). Lietotāji nedrīkst apiet un nesankcionēti lietot aizsargātu Lietotnes funkcionalitāti vai piekļūt Lietotnes datiem.Lietotājiem, pieslēdzoties RSPS pārbaudes laikā, jānodrošina piekļuve RSPS, izmantojot divfaktoru autentifikāciju (2 factor authentication jeb 2FA).RSPS arhitektūrai jābūt izveidotai tā, lai samazinātu potenciālos drošības apdraudējuma riskus. Lietotnē un RSPS jāizveido pietiekami kontroles mehānismi, lai nodrošinātu, ka konfidenciāla informācija, kas uzticēta Lietotnei gan tās pārraides, gan glabāšanas laikā, netiks atklāta personām vai programmām, kurām nav attiecīgas autorizācijas. |
| Lietotāja autentifikācija | Programmatūras izstrādes laikā Piegādātājam ir jāveic programmkoda kvalitātes kontrole, jānodrošina preventīvās un korektīvās darbības. |
| Personas datu uzglabāšana | Datu glabāšanas līmenī personas dati (tālruņa numuri un e-pasta adreses) jāsaglabā šifrētās datu bāzēs (vismaz šifrējot uzglabāšanas laikā – *encrypt at rest*), pēc nepieciešamības atdalot personificētus datus no nepersonificētiem. Personām jānodrošina datu apstrādei noteiktās pamattiesības, t.sk., tiesības lūgt labot vai dzēst datus par šīm personām atbilstoši normatīvajos aktos noteiktiem nosacījumiem un ierobežojumiem. |
| RSPS un Lietotnes atbilstība standartiem un normatīvajiem aktiem | RSPS un Lietotnei jāatbilst:1. 2015. gada 28. jūlija MK noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”;
2. Eiropas Parlamenta un Padomes Regula (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);
3. standartam ISO/IEC 5055:2021.
 |
| RSPS un Lietotnes drošība | Informācijas apmaiņa jānodrošina, izmantojot HTTPS un komerciāli izsniegtus sertifikātus.Izstrādātajam jānodrošina tīmekļa servisa konfigurācija tā, lai servisi, kas paredzēti ierobežotam lietotāju lokam (reģistrētiem un autentificētiem lietotājiem), tiktu darbināti tikai caur šifrētu datu pārraides kanālu.Lietotnei jānodrošina visas tīklā pārraidāmās informācijas šifrēšanu.Lietotnei jānodrošina aizsardzība pret OWASP Top 10 ievainojamībām. |
| Lietotnes drošība | Risinājumam jāveic lietotāja konta bloķēšana, ja tiek izdarīti vairāki (konfigurējams lielums) neveiksmīgi autentifikācijas mēģinājumi. Administratoram ir jāvar veikt lietotāju atbloķēšanu. Jāvar iestatīt atbloķēšanu (aktivēt/izslēgt funkciju) pēc laika (konfigurējams lielums) RSPS sistēmā. |
| Datu dzēšana | 1. Jebkura veida datu dzēšana jāveic tā, lai tā neietekmētu Lietotnes pamatdarbību.
2. Ja lietotājs tiek dzēsts RSPS, tad jānodrošina arī dzēšana Lietotnē.
3. Ja RSPS konstatē, ka Digitālā biļešu sistēmā ir dzēsts lietotājs, tad tiek dzēsts lietotājs atbilstoši šīs sadaļas 2.punktam.
 |

**8.5. Auditācija**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| RSPS darbību auditācija | Jānodrošina auditācijas pierakstu uzkrāšanas funkcionalitāte.Auditēšanas informācija jāglabā tā, lai tā būtu aizsargāta pret jebkādām modifikācijām un to varētu izmantot kā ticamu pierādījumu drošības incidenta izmeklēšanā.RSPS ir jāfiksē un jānodrošina iespēja analizēt individuālā lietotāja (arī administratora) vai citas sistēmas darbības.Piegādātājam jāveic Lietotnes lietotāja darbību auditācijas pierakstus, detalizāciju saskaņojot ar Pasūtītāju, lietotāju pieteikumu izskatīšanas nolūkiem.Auditācijas pieraksti jāglabā 3 mēnešus no to izveidošanas brīža. |
| Notikumu auditācijas pieraksti | RSPS ir jāspēj reģistrēt visus datu apstrādes notikumus, lai sagatavotu nepieciešamās atskaites (lietotāju darbību uzskaite un auditācijas pierakstu veidošana), izpildot Fizisko personu datu aizsardzības likumā noteiktās prasības.RSPS jāspēj izdot atlasītos auditācijas pierakstus mašīnlasāma formā. |
| Kļūdu pārvaldība | Kļūdas – gan serveru, gan servisu, gan aplikācijas u.c. – ir jāuzkrāj auditācijas pierakstos. Kļūdām ir jābūt monitorējamām ar skaidriem kļūdu rašanās cēloņiem. |
| Lietotāja tiesību izmaiņu auditācija | RSPS jāuzglabā un jāvar apskatīt informāciju par visām lietotāju tiesību izmaiņām. Par katru izmaiņu - lietotāja vārds, administratora, kurš veicis izmaiņas, identitāte, izmaiņu datums un laiks, izmaiņu veids (pievienošana, rediģēšanas, dzēšana). |
| Datu izmaiņu vēsture | RSPS ir jāuztur pilna datu izmaiņu vēsture, ja Pasūtītājs nav norādījis citādi. Par katru datu bāzē veikto ieraksta skatīšanos/labošanu/rakstīšanu ir jāizveido auditācijas pieraksts, kā arī labotā/mainītā ieraksta pilnu satura kopiju pirms un pēc labošanas/mainīšanas. |
| Datu dzēšana | Par katru no datu bāzes dzēsto ierakstu ir jāizveido auditācijas pieraksts, kā arī dzēstā ieraksta pilnu satura kopiju pirms dzēšanas. |
| Auditācijas datu eksports | RSPS jānodrošina auditācijas datu (log failu) eksportu uz drošības pārvaldības sistēmu analīzes veikšanai (Azure Sentinel). |

**8.6. Lietojamība**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| Lietotāja saskarņu valoda | Lietotāja saskarnei (izvēlnes, spiedpogas, informatīvie paziņojumi u.c.) jābūt lokalizētai latviešu, angļu un ukraiņu valodā. RSPS administrēšana var būt angļu valodā.  |
| Reaģējošs dizains (responsive design) | Lietotāja saskarnei jānodrošina lietojamība uz dažādu izšķirtspēju ekrāniem. |
| Lietojamība | Lietotnei ir jābūt saprotamai. Visiem lietotāja interfeisa elementiem (navigācijas elementiem, ikonām, spiedpogām, utt.) jābūt viegli uztveramiem un veidotiem atbilstoši industrijas labajai praksei. |
| Lietotāja saskarnes dizains | Lietotāja saskarnē jābūt skaidri norādāmai lietotāja saskarnes videi, nodalot to vizuāli, piemēram, testa videi un produkcijas videi izmantojot dažādas krāsas. |

**8.7. Ieviešana**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| Pirmkoda nodošana | Saskaņā ar 2015. gada 28. jūlija MK noteikumiem Nr. 442, Izstrādātājam nododot Lietotni ekspluatācijā, pēc katras izmaiņas vai uzlabojuma veikšanas Lietotnē un pēc garantijas termiņa beigām, jānodod Pasūtītājam gan programmatūras pirmkods, gan izejas faili (t.sk. kompilēti faili/automatizācijas rīku skripti) par izstrādātajiem programmatūras pielāgojumiem, kas izstrādāti specifiski Pasūtītāja vajadzībām un tā izmantošanas tiesības, iekļaujot visas veiktās izmaiņas.Programmatūras pirmkodam ir jābūt skaidri un precīzi dokumentētiem, tai skaitā programmatūras kodam jāsatur komentāri latviešu vai angļu valodā, kas ir viegli saprotami atbilstošas kvalifikācijas speciālistiem bez pirmkoda autora palīdzības.Programmatūras nodevumu piegādes veids (datu nesējos, Pasūtītāja koda repozitorijā vai citādi) jāsaskaņo ar Pasūtītāju pirms programmatūras piegādes. |
| Lietotāja dokumentācija | Kopā ar risinājumu vai tā komponentēm ir jāizstrādā lietotāja dokumentācija (rokasgrāmata) piegādei nepieciešamā apjomā. |
| Administratora rokasgrāmata | Jānodrošina Lietotnes administratora rokasgrāmatu, kurā tiek vismaz aprakstītas Lietotnes konfigurācijas iespējas. |
| Versiju un konfigurācijas pārvaldība | Lietotnes izstrādes gaitā visām konfigurācijas vienībām un to versijām ir jābūt identificētām, visām izmaiņām trasējamām un sasaistāmām ar konkrētiem darba uzdevumiem un atbildīgajiem.Jaunām nodevumu versijām (gan dokumentiem, gan programmatūrai) jātiek piegādātām atsevišķi, pievienojot izmaiņu vēsturi.Priekšrocība Infrastruktūras piegādei kā kodam (IaC). |
| Testa vide | Izstrādātājam ir jāveic Lietotnes uzstādīšana un konfigurēšana (pielāgošana darbībai konkrētajā vidē) Pasūtītāja infrastruktūrā testa vidē. |
| Produkcijas vide | Pasūtītājs veiks uzstādīšanu un konfigurēšanu produkcijas vidē. Piegādātājam ir jānodrošina savu ekspertu pieejamība konsultācijām par Lietotnes uzstādīšanu un konfigurēšanu. |
| Izstrādes dokumentācija | Izstrādes dokumentu nodevuma pakotnē ietilpst:1. programmatūras prasību specifikācija,
2. programmatūras arhitektūras apraksts,
3. testēšanas plāns, scenāriji, ziņojums,
4. Lietotnes datu bāzu apraksts, to savstarpējā saistītu datu un glabājamo procedūru kopuma apraksts,
5. lietotāju dokumentācija (rokasgrāmata),
6. administratora rokasgrāmata, kurā jābūt aprakstītām arī risinājuma Monitoringa iespējām,
7. darbināšanas, uzturēšanas un atbalsta procedūras,

u.c. dokumentācija pēc nepieciešamības, ja tāda rodas izstrādes laikā.  |
| Laidienu iesniegšanas kārtība | Katra laidiena piegādes ietvaros Piegādātājam jāiesniedz vismaz šāds piegādes nodevumu komplekts:1. izstrādāto programmatūras risinājumu un gatavās programmatūras pielāgojumu pirmkodi, gatavās programmatūras un izstrādāto programmatūras pielāgojumu izpildkodi, konfigurācijas datnes (skripti) piegādei nepieciešamā apjomā;
2. Lietotnes dokumentācijas pirmreizējās vai aktualizētās versijas;
3. datu un/vai datu migrācijas skripti (ja nepieciešams);
4. testu skripti un testa datu kopas, ja nepieciešams;
5. laidiena apraksts,

u.c. dokumentācija pēc nepieciešamības.Dokumenta saturs ir specificējams atkarībā no piegādes apjoma un satura, ievērojot IKT standartus vai vispārpieņemto labo praksi.Piegādātājam nodevuma sagatavošanai jāpiedāvā atbilstoša standarta vai labās prakses metodes (piemēram, [Git](https://github.com/VCTLabs/MIL-STD-498/blob/master/MIL-STD-498-templates-pdf/SVD-DID.PDF)).Pēc noslēgtā iepirkuma līguma vai garantijas termiņa beigām, atkarībā no tā, kas iestājas pirmais Piegādātājam 10 dienu laikā jādzēš viņa rīcībā nonākušos ar līguma izpildi saistītos datus, izņemot gadījumu, ja atkārtoti tiek slēgts līgums ar to pašu pakalpojuma sniedzēju par to pašu līguma priekšmetu. |
| Atvērtā koda risinājumu izmantošana | Projektējot risinājumu, ir vēlams izmantot atvērtā pirmkoda programmatūru. |

1. **Tehniskie un organizatoriskie drošības pasākumi datu aizsardzības nodrošināšanai saskaņā ar Vispārīgo datu aizsardzības regulu (GDPR):**

RP SIA “Rīgas satiksme” ir apņēmusies ievērot zemāk norādītās prasības, tāpēc Lietotnes izstrādātājam ir jāievēro šīs prasības jebkurā no Lietotnes radīšanas procesiem:

* 1. RP SIA “Rīgas satiksme” uzņemas visu atbildību par pārziņā esošās informācijas uzglabāšanu, apstrādi un piegādi atbilstoši Latvijas Republikā spēkā esošajām fizisko personu datu aizsardzības un informācijas un komunikāciju tehnoloģiju drošības prasībām;
	2. RP SIA “Rīgas satiksme” veic pasākumus, lai nodrošinātu, ka jebkura fiziska persona, kas darbojas RP SIA “Rīgas satiksme” pakļautībā un kam ir piekļuve personas datiem, tos apstrādā atbilstoši definētai dalītai pieejai;
	3. RP SIA “Rīgas satiksme” nodrošina, ka personas, kuras ir pilnvarotas apstrādāt personas datus:
		1. apņemas nodrošināt personas datu aizsardzību un konfidencialitāti;
		2. ir apmācītas personas datu aizsardzības jautājumos.
	4. datu apstrādātājs un tā darbinieki pilda šādus pienākumus:
		1. neveido nekādas informācijas vai personas datu kopijas, izņemot tās, kas nepieciešamas, lai izpildītu noteiktu procedūru vai sniegtu pakalpojumu, kas izriet no līguma, vai ar iepriekšēju datu pārziņa piekrišanu;
		2. neizmanto dokumentus un personas datus citiem mērķiem nekā tie, kas izriet no personas datu apstrādes, izņemot normatīvajos aktos noteiktos izņēmumus;
		3. neizpauž dokumentus un informāciju trešajām pusēm, ja vien normatīvajos aktos nav noteiktas tiesības tos saņemt;
		4. veic visu iespējamo, lai nepieļautu personas datu piesavināšanos vai krāpnieciskas darbības ar personas datiem.
	5. RP SIA “Rīgas satiksme” nodrošina integrētās datu aizsardzības un datu aizsardzības pēc noklusējuma principu attiecināšu uz noteiktajām procedūrām unsniegtajiem pakalpojumiem.
	6. RP SIA “Rīgas satiksme” īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, tostarp attiecīgā gadījumā cita starpā:
		1. personas datu pseidonimizāciju un šifrēšanu;
		2. spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību;
		3. spēju laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums;
		4. procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.
	7. RP SIA “Rīgas satiksme” nodrošina visus aizsardzības pasākumus, lai īstenotu personas datu aizsardzību pret jebkādu nejaušu vai nelikumīgu iznīcināšanu, nejaušu zudumu, pārveidošanu, neatļautu izplatīšanu vai pieeju gadījumos, kad personas datu apstrāde ietver datu pārraidi tīklā, kā arī pret jebkuru citu nelikumīgu apstrādes vai komunikācijas ar neautorizētām personām formu.
	8. RP SIA “Rīgas satiksme” nodrošina šādu prasību izpildi:
		1. lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (turpmāk – sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;
		2. katrs reģistrēta lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai (turpmāk – sistēmkonti), tad jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju reģistrētiem lietotājiem izmantot sistēmkontus;
		3. ja netiek izmantota daudzfaktoru autentifikācija, tas ir, viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts, tad reģistrētiem lietotājiem obligāti jālieto paroles;
		4. lietotāja paroles garums nav mazāks par deviņiem simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu vai speciālu simbolu;
		5. lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot šī pielikuma 9.8.7. punktā minēto gadījumu;
		6. lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;
		7. lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
		8. nav pieļaujama funkcionalitāte, kas atļauj lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
		9. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
		10. tiek nodrošināta auditācijas pierakstu veidošana un uzglabāšana par katru piekļuvi informācijas sistēmai, ierakstu, ieraksta labojumu vai dzēšanu ne ilgāk par vienu gadu pēc ieraksta izdarīšanas, ja vien normatīvie akti neparedz garāku glabāšanas termiņu, uzglabājot auditācijas pierakstus vai to kopijas atsevišķi no personas datiem un fiksējot datumu, laiku un personu, kura veikusi personas datu apstrādi;
		11. jebkura piekļuve personas datiem ir izsekojama līdz konkrētam lietotāja kontam vai interneta protokola (IP) adresei;
		12. jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;
		13. visās valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos personas datiem, jābūt iekļautai pretvīrusu funkcionalitātei;
		14. funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām;
		15. katram lietotājam parole ir obligāti jāmaina ne vēlāk kā pēc 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;
		16. lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām lietotāja parolēm;
		17. piecas secīgas reizes nepareizi ievadot lietotāja konta paroli, šis konts (izņemot administratora kontu) nekavējoties tiek bloķēts;
		18. ar administratora kontu piekļūt personas datiem, izmantojot iekārtas, kas atrodas ārpus RP SIA “Rīgas satiksme” telpām, kā arī iekārtas, kas neatrodas RP SIA “Rīgas satiksme” valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju;
		19. fiziski piekļūt iekārtām atļauts vienīgi pilnvarotām personām;
		20. auditācijas pieraksti tiek veidoti, nodrošinot, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar vienas sekundes precizitāti;
		21. tiek nodrošināta auditācijas pierakstu satura plānveida uzraudzība un analīze, lai konstatētu drošības incidentus;
		22. lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai lietotājs pašrocīgi vai ar atbalsta personāla palīdzību atrisinātu kļūdu;
		23. plūsma starp personas datiem un tās lietotājiem, kā arī starp personas datu apstrādes sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri;
		24. datortīkla pakalpojumi (network services), kas netiek izmantoti personas datu apstrādes sistēmas darbības nodrošināšanai, ir atslēgti;
		25. veicot izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu glabāto personas datu integritātei;
		26. personas datu izvietošana ārpakalpojuma sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un personas dati atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.
	9. RP SIA “Rīgas satiksme” veido personas datu rezerves kopijas, nodrošinot pakalpojumu nepārtrauktību.
	10. RP SIA “Rīgas satiksme” izstrādā informācijas resursu atjaunošanas plānu.
	11. RP SIA “Rīgas satiksme”, novērtējot atbilstīgo drošības līmeni, ņem vērā jo īpaši riskus, ko rada apstrāde, jo īpaši nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.
1. **RSPS garantija un pieteikumu apstrādes vadlīnijas:**

10.1. Garantija:

* + 1. Piegādātājs uztur garantiju 2 (divus) gadus no  nodošanas - pieņemšanas akta parakstīšanas brīža. Garantiju Piegādātājs realizē termiņos saskaņā ar tehniskajā specifikācijā noteikto, pilnībā novēršot garantijas pieteikumā fiksētās problēmas un/vai nepilnības, tai skaitā kļūdas par saviem līdzekļiem un saviem spēkiem;
		2. Piegādātājs nodrošina garantiju, atbilstoši un ievērojot ITIL ITSM (Support level) vadlīnijas ar specifiskām pieteikumu kategorijām un to prioritātēm. (Garantija ietver 2., 3. un 4. kategorijas pieteikumus – kļūdas un neprecizitātes).
	1. Pieteikumu apstrādes vadlīnijas:
		1. Piegādātājs nodrošina pieteikumu, problēmu un bojājumu centralizētu apstrādi attiecībā uz līguma darbības laikā izstrādātiem nodevumiem 24 stundas dienā 7 dienas nedēļā šādos kanālos:
			1. zvaniem uz norādītu kontakttālruni (2. kategorijas gadījumos);
			2. elektronisku vēstuļu sūtījumiem uz norādītu e-pasta adresi.
		2. Pieteikuma saņemšanas brīdī reģistrē Piegādātājs Pieteikumu sistēmā tā pieteikšanas laiku un sniedz reģistrācijas apstiprinājumu, nosūtot atbildes e-pasta paziņojumu.
		3. Piegādātājs nodrošina Pasūtītājam piekļuvi Piegādātāja Pieteikumu sistēmā reģistrētajiem Pasūtītāja pieteikumiem.
		4. Pieteikumu apstrādi nodrošina šādā darba režīmā:
			1. visu kategoriju pieteikumiem, izņemot 2. kategorijas gadījumos, katru darba dienu laikā no plkst.07:00 līdz 16:30;
			2. lēmumu pieņemšanu par pieteikumu kategorijas maiņu no zemākas uz 2.kategoriju un tā izpildes uzsākšanu ārpus pamata darba veic tikai Pasūtītājs.
		5. Piegādātājs nodrošina pieteikto problēmu novēršanu un/vai uzdevumu apstrādi Piegādātājs veic saskaņā ar tehniskajā specifikācijā noteikto darba režīmu un ievērojot šādus minimālos reakcijas, pagaidu risinājuma un pilnas novēršanas laikus:
			1. reakcijas laiks ir – laika periods no pieteikuma saņemšanas, kad ir sniegta vai reģistrēta pilna apjoma pieteikuma informācija, brīža līdz brīdim, kad tiek iesniegta reakcijas laika atbilde, kurā iekļauj vismaz šādu informāciju: izskaidrots problēmas cēlonis (ja tas ir zināms), izskaidrots veids, kā tiks novērsta un atrisināta problēma, vai sniegta informācija, pagaidu risinājuma ieviešanas un/vai novēršanas laiks un/vai plāns, nepieciešamās un/vai veicamās darbības, kas palīdzētu problēmu lokalizēt vai minimizēt tās ietekmi;
			2. pastāvīgā risinājuma piegādes mērķa termiņš vai atrisināšanas laiks un pagaidu risinājuma piegādes mērķa termiņš – ir laika periods no reakcijas laika atbildes saņemšanas un apstiprināšanas brīža, līdz brīdim, kad pakalpojumu sniedzējs ir nodrošinājis risinājumu, pēc kura vairs nav iespējams atkārtot pieteikto problēmu, vai arī ir veicis darbības, kas samazina attiecīgā pieteikuma kategoriju uz zemāku;
			3. reakcijas laiks **2. kategorijas** pieteikumam ir ne ilgāk kā 4 stundas ar pagaidu risināšanas darba izpildi 8 stundu laikā un pastāvīga risinājuma piegādi ne ilgāk kā 24 stundu laikā;
			4. reakcijas laiks **3. kategorijas** pieteikumam ir ne ilgāk kā 8 stundas ar pagaidu risināšanas darba izpildi 24 stundu laikā un pastāvīga risinājuma piegādi ne ilgāk kā 48 stundu laikā;
			5. reakcijas laiks **4. kategorijas** pieteikumam ir ne ilgāk kā 2 darbdienas ar pastāvīga risinājuma piegādi ne ilgāk kā 3 darbdienas.