Pielikums Nr.11

**1. Kiberdrošības atbilstība un drošības audita prasības**

**1.1 Kiberdrošības standartu ievērošana**

Piegādātājam jānodrošina, ka visi piegādātie elektriskie transportlīdzekļi (ETL), iebūvētās elektroniskās vadības ierīces (EVI), telemātikas ierīces, programmatūras platformas un saistītā uzlādes infrastruktūra atbilst šādiem kiberdrošības standartiem:

* ISO/SAE 21434:2021 — Ceļu transportlīdzekļu kiberdrošības inženierija;
* ETSI EN 303 645 — Kiberdrošība patērētāju lietu interneta ierīcēm;
* Attiecīgās ANO EHK (UNECE) WP.29 kiberdrošības regulas (Regula Nr. 155) prasības.

Pretendenta komentārs:

**1.2 Drošības auditi**

* Piegādātājam jāiesniedz pasūtītājam kiberdrošības audita ziņojums, kas apstiprina atbilstību minētajiem standartiem.
* Auditu veic sertificēta trešā puse.

Pretendenta komentārs:

* 1. **Ziņošana par incidentiem**
* Par jebkuru drošības incidentu, kas saistīts ar ETL sistēmām, piegādātājam jāziņo pasūtītājam 24 stundu laikā pēc incidenta atklāšanas. Detalizēts drošības incidenta ziņojums jāiesniedz 5 darba dienu laikā.
* Par personas datu aizsardzības incidentiem piegādātājam jāziņo nekavējoties, bet ne vēlāk kā 24 stundu laikā pēc incidenta atklāšanas, ziņojumā norādot visu informāciju, kas saistīta ar incidentu

Pretendenta komentārs:

**2. Personas datu aizsardzība**

**2.1 Atbilstība personas datu aizsardzības normatīvajiem aktiem**

Piegādātājam jānodrošina personas datu apstrāde saskaņā ar:

* Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (Vispārīgā datu aizsardzības regula — GDPR);
* Fizisko personu datu apstrādes likumu.
* un citiem normatīvajiem aktiem, kas regulē personas datu apstrādi un aizsardzību

Pretendenta komentārs:

**2.2 Personas datu apstrādes vieta**

* Personas datu apstrāde ETL sistēmās un lietojumprogrammās notiek Eiropas Ekonomikas zonā (EEZ).
* Datu apstrāde ārpus EEZ ir atļauta tikai ar pasūtītāja rakstisku atļauju un saskaņā ar GDPR 46. panta prasībām.

Pretendenta komentārs:

**2.3 Personas datu plūsmas dokumentācija**

Piegādātājam jāiesniedz datu plūsmas karte, kurā skaidri norādīti:

* Savāktie datu veidi;
* Datu glabāšanas un pārsūtīšanas punkti;
* Trešo personu un apakšapstrādātāju (apakšuzņēmēju) piekļuve un lomas;
* Datu glabāšanas un dzēšanas politikas.

Pretendenta komentārs:

**2.4 Personas datu drošības pasākumi**

* Dati jāšifrē, izmantojot AES-256 vai augstāku standartu un TLS 1.2 vai 1.3 protokolus.
* Visām mākoņpakalpojumu un lietojumprogrammu piekļuves sistēmām jābūt aprīkotām ar drošu autentifikāciju (piemēram, divfaktoru autentifikāciju).

Pretendenta komentārs:

**2.5 Personas datu apstrādes izbeigšana līguma termiņa beigās**

* Līguma beigās vai tā pārtraukšanas gadījumā piegādātājam jānodrošina:
	+ Datu nodošana pasūtītājam drošā, šifrētā formātā;
	+ Droša visu datu, ieskaitot dublējumus, dzēšana.

Pretendenta komentārs:

**3. Audita tiesības un atbilstības uzraudzība**

Pasūtītājam ir tiesības:

* Veikt regulārus vai ārkārtas auditus par piegādātāja kiberdrošības un personas datu apstrādes procesu atbilstību;
* Uzlikt līgumsodu vai izbeigt līgumu, ja atbilstības prasības netiek ievērotas.

Pretendenta komentārs: