	Bezpečnostní opatření	Popis bezpečnostních opatření zavedených zprostředkovatelem
1.	**Opatření zaměřená na pseudonymizaci a šifrování osobních údajů**	Všechny pracovní stanice a servery podléhají jednotnému bezpečnostnímu standardu, který zahrnuje antivirovou ochranu, ochranu EDR, místní firewall, IPS/IDS, šifrování úložiště a další vrstvy včetně nastavení operačního systému, segmentace sítě a fyzické bezpečnosti. Při exportu dat pro analytické účely se používá anonymizace.
2.	**Opatření k zajištění trvalé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování dat.**	Přístup k datům je řízen na základě zásady "need-to-know". Přístupová práva jsou nastavena na několika úrovních - uživatelská oprávnění a přístup k síti. Data jsou uložena v profesionálním datovém centru s nepřetržitým zabezpečením a certifikací ISO 27002. Fyzický přístup je omezen na oprávněné pracovníky a je monitorován a auditován.
3.	**Opatření k zajištění schopnosti včas obnovit dostupnost a přístup k osobním údajům v případě fyzického nebo technického incidentu.**	Pravidelné zálohování s geografickou redundancí; obnova je pravidelně testována. Zálohování se provádí prostřednictvím centrálního zálohovacího systému. Přístup k němu mají pouze oprávněné osoby. Zálohy jsou uloženy tak, aby byly k dispozici i v případě výpadku primárního pracoviště.
4.	**Procesy pravidelného testování, posuzování a hodnocení účinnosti technických a organizačních opatření k zajištění bezpečnosti zpracování.**	Všechna přijatá bezpečnostní opatření jsou pravidelně interně i externě testována v rámci certifikace ISO 27001 a také v souladu s požadavky amerického zákona Sarbanes-Oxley. Certifikát ISO 27001:2022 potvrzuje platnost systému ISMS pro všechna data klientů, společností a dodavatelů, včetně transakčních a osobních údajů v oblasti paliv a dopravy.
5.	**Opatření k identifikaci uživatelů a poskytování uživatelských oprávnění**	Vícefaktorová autentizace, systém rolí a audit přístupu k datům.
6.	**Opatření na ochranu dat při přenosu**	Data z telematických zařízení jsou při leteckém přenosu šifrována (GEA-3, LLC) a směrována přes soukromé APN a soukromou linku. Ačkoli se nepoužívá šifrování na aplikační vrstvě, vzhledem k proprietárnímu protokolu a kompresi nejsou data čitelná. Toto řešení zajišťuje bezpečný přenos v souladu s článkem 32 nařízení GDPR.

7.	**Opatření na ochranu údajů při ukládání**	Data jsou v databázích šifrována a ukládána v prostorách s omezeným přístupem.
8.	**Opatření k zajištění fyzické bezpečnosti míst, kde se zpracovávají osobní údaje**	Přístup do fyzických míst je omezen na oprávněné osoby a přístup je monitorován a zaznamenáván.
9.	**Opatření k zajištění zaznamenávání událostí**	Zaznamenávání přístupů a operací v systému, přičemž protokoly se uchovávají v souladu s pravidly uchovávání.
10.	**Opatření k zajištění konfigurace systému, včetně výchozí konfigurace**	Předvolby bezpečné konfigurace, zásada nejmenších oprávnění vyžadovaná při nasazení systému.
11.	**Vnitřní správa IT a opatření pro bezpečnost IT**	Zavedený systém řízení bezpečnosti informací ISO 27001, interní směrnice a školení. Ochrana IT systémů je řízena centrálně na úrovni skupiny prostřednictvím oddělení informační bezpečnosti. Pro každou oblast bezpečnosti informací byly stanoveny interní standardy, které jsou pravidelně aktualizovány, aby odrážely aktuální vývoj. Dodržování těchto standardů je povinné a je centrálně sledováno.
12.	**Opatření k certifikaci/zabezpečení procesů a produktů**	Certifikace ISO 27001, pravidelná aktualizace dokumentace a auditovaných procesů.
13.	**Opatření k zajištění minimalizace údajů**	Shromažďujeme pouze údaje nezbytné pro poskytování služby.
14.	**Opatření týkající se kvality dat**	Automatické a manuální kontroly, detekce anomálií.
15.	**Opatření k zajištění omezeného uchovávání údajů**	Zásady uchovávání údajů v souladu s GDPR.
16.	**Opatření k zajištění odpovědnosti**	Vedení záznamů o činnostech zpracování, pověřenec pro ochranu osobních údajů (DPO).
17.	**Opatření umožňující přenositelnost údajů a zajišťující výmaz.**	Funkce pro export dat ve standardizovaných formátech, bezpečný mechanismus pro výmaz dat.
18.	**V případě předávání jiným zpracovatelům popište také konkrétní technická a organizační opatření, která má jiný zpracovatel přijmout, aby poskytl správci pomoc.**	Smlouvy musí obsahovat bezpečnostní požadavky.

19.	**Popis konkrétních technických a organizačních opatření, která má zpracovatel přijmout, aby mohl správci poskytnout pomoc.**	Zavedené procesy pro žádosti subjektů údajů, hlášení incidentů a poskytování dokumentace.
20.	**Opatření pro řízení bezpečnostních incidentů**	Zavedený rámec pro bezpečnost informací a incidentů s údaji - hlášení a řízení, který zahrnuje proces identifikace, klasifikace a řešení bezpečnostních incidentů pod vedením oddělení bezpečnosti informací.