PŘÍLOHA 1

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ K ZABEZPEČENÍ OCHRANY OSOBNÍCH ÚDAJŮ

1. Zákonné povinnosti zpracovatele

1.1 Zpracovatel je povinen:

(a) zabránit neoprávněným osobám přistupovat k Osobním údajům a k prostředkům pro jejich zpracování;

(b) zabránit neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících Osobní údaje;

(c) přijmout opatření, která umožní určit a ověřit, komu byly Osobní údaje předány; a

(d) přijmout pokyny stanovující pravidla pro přístup a další zpracování Osobních údajů.

1.2 V oblasti automatizovaného zpracování Osobních údajů je Zpracovatel povinen také:

(e) zajistit, aby systémy pro automatizovaná zpracování Osobních údajů používaly pouze oprávněné osoby;

(f) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování Osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;

(g) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly Osobní údaje zaznamenány nebo jinak zpracovány; a

(h) zabránit neoprávněnému přístupu k datovým nosičům.

2. Konkrétní opatření Zpracovatele k zabezpečení ochrany Osobních údajů

2.1 Fyzický přístup

Zpracovatel dodržuje standardy fyzického zabezpečení navržené za účelem zabránění neoprávněnému fyzickému přístupu k zařízení a vybavení Zpracovatele. To je provedeno následujícími opatřeními:

- fyzický přístup na místa je omezen na zaměstnance Zpracovatele, jeho subdodavatele a povolené návštěvy;

2.2 Kontrola přístupu a správa

Zpracovatel dodržuje následující standardy kontroly přístupu a správy příslušného IT prostředí:

- účty správce (administrátora) by měly být užívány pouze pro účely výkonu správcovských činností;
- každý účet s oprávněními správce musí být spojitelný s jedinečně identifikovatelnou osobou;

- veškeré přístupy k počítačům a serverům musí být ověřovány a používány v rámci výkonu pracovní pozice zaměstnance;
- hesla musí být jednoznačně přiřaditelná k určité osobě;
- délka hesla musí být nastavena nejméně na 8 znaků;
- musí být nastaveno automatické odhlášení z počítače a serveru při nečinnosti s nutností znovu zadat heslo k ověření;

2.3 Kontrola virů a záznamy

Počítače a servery obsahují odpovídající aktuální verze softwarů pro monitorování zabezpečení systémů, které zahrnují host firewall, antivirovou ochranu a aktuální rozpoznávání ohrožujících softwarů a virů. Takový software je nastaven na vyhledání a okamžité odstranění nebo nápravu identifikovaných nálezů.

Zpracovatel vede záznamy o různých částech infrastruktury a systému detekce průniku za účelem monitorování, vyhledávání a reportování vzorců zneužití, podezřelých činností, neoprávněných uživatelů a jiných skutečných anebo hrozících bezpečnostních rizik.

2.4 Pracovníci Zpracovatele

Zaměstnanci Zpracovatele a osoby pracující pro Zpracovatele na základě smlouvy jsou vyškoleni ohledně pravidel Zpracovatele týkajících se bezpečnosti a ochrany soukromí a jsou upozorněni na jejich odpovědnost v souvislosti se zásadami ochrany soukromí a bezpečnosti.

Zaměstnanci Zpracovatele a osoby pracující pro Zpracovatele na základě smlouvy jsou smluvně vázáni zachovávat mlčenlivost o Osobních údajích nebo důvěrných informacích a dodržovat příslušné interní předpisy, standardy nebo požadavky Zpracovatele týkající se zpracování Osobních údajů. Nedodržení těchto interních předpisů, standardů nebo požadavků bude předmětem šetření, které může vyústit až v disciplinární řízení včetně ukončení pracovního poměru nebo spolupráce se Zpracovatelem.

Zaměstnanci Zpracovatele a osoby pracující pro Zpracovatele na základě smlouvy mají přístup pouze k těm Osobním údajům, které nezbytně potřebují v souladu s pravidly přístupu obsaženými ve článcích 2.1 a 2.2 výše.