

Príloha č. 4 – Bezpečnostné opatrenia

1. Úvodné ustanovenia

Táto príloha stanovuje minimálne technické a organizačné požiadavky v oblasti ochrany osobných údajov, informačnej a kybernetickej bezpečnosti, ktoré je Partner povinný dodržiavať pri plnení tejto Zmluvy, Prílohy č. 5, t.j. pri spracúvaní osobných údajov ako sprostredkovateľ podľa GDPR.

2. Organizačné opatrenia

2.1 Partner je povinný určiť zodpovednú osobu za informačnú a kybernetickú bezpečnosť.

2.2 Partner je povinný zaviesť a udržiavať vnútorné/interné bezpečnostné politiky minimálne v oblastiach:

- riadenia prístupových práv k systémom, údajom a osobným údajom,
- zaobchádzania s incidentmi (detekcia, oznamovanie, riešenie),
- bezpečnosti prevádzky IT systémov a správy zmien,
- školenia zamestnancov v oblasti ochrany údajov a informačnej bezpečnosti.

2.3 Všetci zamestnanci Partnera, ktorí manipulujú s osobnými údajmi alebo majú prístup k systémom, musia byť preukázateľne zaškolení a poučení v oblasti ochrany údajov a kybernetickej bezpečnosti a musia mať podpísané „Vyhlásenie o oboznámení a mlčanlivosti“ v zmysle článku 14 Zmluvy.

2.4 Partner vedie aktuálnu evidenciu oprávnených osôb, ktoré majú prístup k údajom a evidenciu k „Vyhláseniam o oboznámení a mlčanlivosti“.

3. Technické opatrenia

3.1 Prístup do systémov, vrátane Aplikácie, musí byť vždy zabezpečený:

- autentifikáciou menom a heslom, pričom heslá sa pravidelne menia,
- dvojfaktorovou autentifikáciou, ak to technické riešenie umožňuje.

3.2 IT zariadenia používané na Predajných miestach musia byť vybavené:

- aktuálnym antivírusovým softvérom a firewallom,
- automatizovaným systémom aktualizácií (OS aj aplikácií),
- šifrovaním disku (v prípade ukladania údajov na lokálne zariadenia),
- nastavením zabezpečeného prístupu (napr. automatickým uzamykaním obrazovky).

3.3 Prenos osobných údajov a transakčných dát medzi Predajnými miestami a Centrálnym systémom musí prebiehať výlučne cez šifrovaný komunikačný kanál (napr. HTTPS, VPN).

3.4 Prístup do Aplikácie musí byť logovaný, vrátane evidencie zmien a úkonov nad údajmi.

3.5 Tlač potvrdení a daňových dokladov nesmie obsahovať nadbytočné osobné údaje.

3.6 Lokálne ukladanie osobných údajov mimo Aplikáciu je zakázané.

4. Fyzické opatrenia

4.1 Zariadenia používané na Predajných miestach musia byť fyzicky chránené pred:

- neoprávneným prístupom alebo manipuláciou,
- odcudzením a poškodením (vrátane náhodného ako je napr. požiar alebo záplavy).

4.2 Neoprávneným osobám nesmie byť umožnený prístup k žiadnej časti systému alebo zariadeniam, ktoré sú súčasťou Projektu.

5. Monitorovanie, audit a reakcia na incidenty

- 5.1 Partner vedie záznamy o prístupoch k systémom a manipulácii s údajmi.
- 5.2 Objednávateľ je oprávnený vykonať bezpečnostný audit alebo kontrolu dodržiavania podmienok Zmluvy vrátane všetkých príloh a/alebo preukázateľných pokynov Objednávateľa vo vzťahu k spracúvaniu údajov.
- 5.3 V prípade bezpečnostného incidentu alebo narušenia ochrany osobných údajov je Partner povinný bezodkladne, najneskôr do 24 hodín od zistenia, informovať Objednávateľa.
- 5.4 Partner je povinný dokumentovať prijaté nápravné opatrenia a riadiť sa pokynmi Objednávateľa.

6. Pravidelné preverovanie a zlepšovanie

- 6.1 Partner je povinný najmenej raz ročne vykonať interné preverenie súladu so Zmluvou, jej prílohami a aktuálnymi pokynmi Objednávateľa, ako aj vyhodnotiť účinnosť prijatých opatrení.
- 6.2 Na požiadanie Objednávateľa je Partner povinný predložiť správu o stave bezpečnosti.

7. Záverečné ustanovenia

- 7.1 V prípade rozporu medzi týmito opatreniami a platnými právnymi predpismi ako napríklad GDPR, sa uplatní ten režim, ktorý poskytuje vyššiu úroveň ochrany.
- 7.2 Partner zabezpečí, že rovnaké bezpečnostné opatrenia budú uplatňované aj všetkými zamestnancami Partnera, ktorí spracúvajú osobné údaje v rámci plnenia tejto Zmluvy.