Príloha č. 1 k Vnútornému predpisu – Pravidlá ochrany osobných údajov – Dokumentácia o technických a organizačných bezpečnostných opatreniach softvéru EuroSecom

Prevádzkovateľ softvéru:
COEX spol. s r.o., so sídlom: Sotinská 1474/11, 905 01 Senica, IČO: 17 330 581 , zapísaný v Obchodnom registri Okresného súdu Trnava, odd. Sro, vložka č. 40152/T

1.Technické opatrenia

1.1.Technické opatrenia realizované prostriedkami fyzickej povahy

Osobné údaje sú spracovávané na osobných počítačoch umiestnených v uzamknutých kanceláriách chránených v mimopracovnej dobe elektrickým zabezpečovacím systémom objektu. Objekty s počítačmi, na ktorých sa spracovávajú osobné údaje sú chránené pred fyzickým prístupom neoprávnených osôb. Fyzické nosiče osobných údajov (napr. listinné dokumenty) sú bezpečne uložené v uzamykateľných skriniach. Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému je zaistené vhodným umiestnením zobrazovacích jednotiek. Nepotrebné fyzické nosiče osobných údajov sú zničené v zariadení na skartovanie listín.

1.2. Ochrana pred neoprávneným prístupom

Pri prenose a premiestňovaní osobných údajov sa používa 128 bitová šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí.

1.3 Riadenie prístupu oprávnených osôb

Identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme je vyriešená prostredníctvom prístupu do informačného systému cez šifrované heslo a GRID kód. Každý vstup jednotlivých oprávnených osôb do informačného systému je zaznamenaný do tabuľky prístupov.

1.4 Ochrana proti škodlivému kódu

Antivírový program zabezpečuje detekciu prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov na každom počítači, na ktorom sú spracovávané osobné údaje. Antivírový program zabezpečuje ochranu pred nevyžiadanou elektronickou poštou. Na všetkých počítačoch, na ktorých sú spracovávané osobné údaje sa používa len legálny a prevádzkovateľom schválený softvér.

1.5 Sieťová bezpečnosť

Prepojenie informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou prebieha šifrovanou komunikáciou a prístup je chránený šifrovaným heslom a GRID kódom. Všetky miesta prepojenia sietí s verejne prístupnou počítačovou sieťou sú evidované. Vnútorné prostredie kancelárie, kde prebieha spracovanie osobných údajov je

zabezpečené prostredníctvom nástroja sieťovej bezpečnosti firewall. Komunikácia na verejne prístupnej počítačovej sieti je monitorovaná pre zabezpečenie ochrany proti iným hrozbám pochádzajúcich z verejne prístupnej počítačovej siete (napr. hackerský útok).

1.6 Zálohovanie

Zálohy informačného systému sú testované na funkcionalitu dátového nosiča zálohy po každom zálohovaní, ktoré prebieha s vopred zvolenou periodicitou. Súčasťou testu je aj test obnovy informačného systému zo zálohy. Zálohy sú uložené na šifrovaných nosičoch v uzamykateľných skriniach v priestoroch monitorovaných elektronickým bezpečnostným zariadením.

1.7 Likvidácia osobných údajov a dátových nosičov

Z nepoužívaných nosičov osobných údajov sa najprv bezpečne vymažú osobné údaje a následne sa zlikvidujú v zariadení na skartovanie dátových nosičov osobných údajov.

1.8 Aktualizácia operačného systému a programového aplikačného vybavenia

Aktualizácia operačného systému a programového aplikačného vybavenia prebieha vo vopred dohodnutých termínoch pri odhlásení všetkých užívateľov informačného systému pre spracovanie osobných údajov.

2. Organizačné opatrenia

2.1 Personálne opatrenia

Všetky oprávnené osoby, ktoré pracujú s informačným systémom boli písomne poučené pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi. Všetky oprávnené osoby sú poučené o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie, dostali vymedzené osobné údaje, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh. Všetky oprávnené osoby dostali určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov, vymedzenie zakázaných postupov alebo operácií s osobnými údajmi a vymedzenie zodpovednosti za porušenie zákona. Oprávnené osoby sú poučené o postupoch spojených s automatizovanými prostriedkami spracúvania a o súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov). Oprávnené osoby sú oboznámené s bezpečnostnými smernicami. Pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby táto odovzdá pridelené aktíva, zrušia sa prístupové práva, a vykoná sa poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti.

2.2 Vedenie zoznamu aktív a jeho aktualizácia

O všetkých aktívach a právach k informačnému systému je vedená písomná evidencia.

2.3 Riadenie prístupu oprávnených osôb k osobným údajom

Vstup do objektu, kde prebieha spracovanie osobných údajov je kontrolovaný prevádzkovateľom prostredníctvom technických a personálnych opatrení. Rezervné kľúče k objektom sú bezpečne uložené v uzamykateľnej skrini. Prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb a správa hesiel je evidovaná a pravidelne kontrolovaná. Je

zabezpečené vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru).

2.4 Organizácia spracúvania osobných údajov

Osobné údaje sú spracovávané v chránenom priestore a je zabezpečená nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby vrátane doby údržby a upratovania chránených priestorov. Osobné údaje nie sú spracovávané mimo chráneného priestoru, Neprebieha manipulácia s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti. Pri používaní automatizovaných prostriedkov spracúvania (napr. notebooky) v chránených priestoroch je stanovená zodpovednosť oprávnenej osoby za ochranu osobných údajov. Prenosné dátové nosiče sa nepoužívajú mimo chránených priestorov.

2.5 Likvidácia osobných údajov

V prípade likvidácie osobných údajov sa osobný údaj bezpečne vymaže z dátového nosiča bez možnosti dodatočnej obnovy osobného údaja zo zálohy. Nepotrebné fyzické dátové nosiče sa zlikvidujú zariadením na skartáciu. Za proces bezpečnej likvidácie sú zodpovedné oprávnené osoby.

2.6 Bezpečnostné incidenty

V prípade bezpečnostných incidentov a zistených zraniteľných miest informačného systému treba okamžite tieto prípady ohlásiť na účel včasného prijatia preventívnych alebo nápravných opatrení. Bezpečnostné incidenty sa zaznamenávajú v Evidencii bezpečnostných incidentov a použitých riešení. Pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača) je treba vždy prítomnosť oprávnenej osoby.

2.7 Kontrolná činnosť

Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení sa bude vykonávať raz za týždeň so zameraním na kontroly prístupov k informačnému systému. O výsledkoch kontroly budú informované oprávnené osoby.

Názov Softvéru	EuroSecom – internetový ekonomický softvér
Prístup do softvéru	Prístupové meno a heslo a GRID karta so šifrovanou komunikáciou
Predajca softvéru	Licencia 2018 od spololočnosti COEX spol. s r. o.
Mzdový program je automatizovaný informačný systém typu klient - server	ÁNO
Server je pripojený na zdroj záložného napájania UPS	ÁNO
Umiestnenie servera	Virtuálny server
Operačný systém servera	Linux
Zálohy IS dát zo servera sú realizované	Denne v týždennom cykle na zálohovací virtuálny server