SLUŽBY SPOLOČNOSTI WORLDLINE PRE OBCHODNÍKOV

Technické a organizačné

opatrenia

1. ÚČEL TOHTO DOKUMENTU

Tento dokument obsahuje zoznam technických a organizačných opatrení, ktoré sa štandardne uplatňujú. Reálne prijaté opatrenia závisia od služby a miesta príslušného spracúvania, keďže nie všetky opatrenia sú relevantné pre všetky služby a miesta. Spoločnosť Worldline ručí za to, že má pre všetky služby a miesta nevyhnutné primerané technické a organizačné opatrenia zahrnuté v nižšie uvedenom zozname. Opatrenia sú navrhnuté na účely:

- zabezpečenia bezpečnosti a dôvernosti Osobných údajov;
- ochrany proti akýmkoľvek predpokladaným hrozbám alebo nebezpečenstvám vo vzťahu k bezpečnosti a integrite Osobných údajov;
- ochrany proti akémukoľvek skutočnému neoprávnenému spracovaniu, strate, používaniu, poskytnutiu alebo získaniu prístupu k akýmkoľvek Osobným údajom.

Spoločnosť Worldline sa zaväzuje priebežne monitorovať účinnosť svojich opatrení na ochranu informácií. Spoločnosť Worldline sa zaväzuje naďalej dodržiavať PCI DSS [1].

2. TECHNICKÉ A ORGANIZAČNÉ OPATRENIA

A. Osoby, povedomie a ľudské zdroje (HR):

- Pri každom najímaní pracovníkov sa dodržiava proces previerky podľa zásad bezpečnostnej previerky skupiny Worldline, a to v rámci obmedzení miestnych právnych predpisov;
- V každej zmluve má každý zamestnanec doložky o dohode o zachovaní mlčanlivosti;
- Všetci pracovníci sú povinní každoročne absolvovať školenie v oblasti povedomia o Etickom kódexe (vrátane testu);
- Pracovníci spoločnosti Worldline sú povinní každý rok absolvovať školenie spoločnosti Worldline v oblasti ochrany údajov, školenie v oblasti informačnej bezpečnosti a bezpečnosti a školenie PCI DSS v oblasti bezpečnosti, a následne zo všetkých absolvovať test
- Všetkým zamestnancom je poskytnuté Vyhlásenie o zásadách bezpečnosti a Zásady ochrany údajov;
- Zamestnanci sú povinní dodržiavať platné miestne bezpečnostné zásady a zásady ochrany údajov, ako aj bezpečnostné zásady a zásady ochrany údajov skupiny Atos a Worldline;
- Pravidelná komunikácia zameraná na informovanosť o nariadení GDPR pre všetkých pracovníkov (okrem školení Worldline v oblasti zásad ochrany údajov, informačnej bezpečnosti a v oblasti bezpečnosti);
- Dodatočné špecifické školenia ponúkané subjektmi na ochranu údajov pre vybrané tímy a zamestnancov.

B. Organizačná kontrola

Spoločnosť Worldline si bude udržiavať svoju internú organizáciu spôsobom, ktorý spĺňa požiadavky platných právnych predpisov a požiadavky prevádzkovateľa údajov na bezpečnosť údajov. To je možné dosiahnuť:

- Vymenovaním zástupcu pre ochranu údajov
- Zavedením ochrany údajov, bezpečnosti a organizácie a riadenia kontinuity činnosti
- Širokou sieťou odborníkov na ochranu údajov v rámci Atos a Worldline
- Úlohami a zodpovednosťami v oblasti ochrany údajov pre všetkých pracovníkov
- Súborom zásad na riadenie ochrany a bezpečnosti údajov
- Internými zásadami, postupmi a procesmi spracovania údajov pre kódovanie, testovanie, zmeny a zverejnenia, pokiaľ sa týkajú spracúvaných Osobných údajov;

[1] PCI DSS: Odvetvie priemyselných kariet – Norma o bezpečnosti údajov – týka sa ochrany údajov držiteľov kariet.

- Zavedením kontrolného rámca Ochrany údajov, pomocou ktorého sa pravidelne vyhodnocuje súlad
- Vykonávaním pravidelných interných bezpečnostných auditov s cieľom overiť bezpečnostné postupy.
- Zabezpečením toho, aby sa na dodávateľov spracúvajúcich osobné údaje vzťahovali rovnaké technické a organizačné opatrenia

C. Fyzická bezpečnosť a záznamy v tlačenej podobe:

Všetky subjekty v rámci Skupiny dodržiavajú Zásady fyzickej a environmentálnej bezpečnosti a Normu ochrany informácií skupiny Worldline:

- kontrola fyzického prístupu sa vykonáva u všetkých zamestnancov a vo vzťahu ku všetkých návštevníkom/hosťom sa implementujú systémy riadenia návštev;
- kontroly fyzického prístupu podľa definovanej periodicity;
- informácie, ktoré zahŕňajú tlačené dokumenty, sú klasifikované, označené, chránené a spracúvané v súlade so zásadami spoločnosti Worldline pre klasifikáciu informácií;
- konkrétne pravidlá definujú spôsob uchovávania, spracúvania, zobrazovania, tlače, prenášania a likvidácie (v elektronickej, ako aj papierovej forme);
- kamerové systémy CCTV na ochranu oblastí s obmedzeným vstupom;
- je zavedená protipožiarna ochrana, protipovodňová ochrana, vykurovanie, klimatizácia, záložné zdroje energie, aby sa zabezpečila integrita a dostupnosť údajov uchovávaných v dátových centrách;
- kontrolovaná likvidácia dátových médií.

D. Technická infraštruktúra a bezpečnosť aplikácií:

Spoločnosť Worldline zaviedla ochranu v prísne zabezpečenom prostredí, ktoré zabezpečuje viaceré bezpečnostné úrovne. Sú zavedené nasledujúce bezpečnostné opatrenia:

- segregácia a segmentácia siete;
- zabezpečený prenos dát cez neznáme siete;
- osobné údaje uchovávané v produkčných sieťach, ktoré sú oddelené prostredníctvom firewall;
- IDS (Intrusion Detection) a IPS (Intrusion Prevention) – a monitorovanie (SIEM – Security Information and Event Management System);
- bezpečnostné brány a riešenie VPN na zabezpečenie prístupu na diaľku;
- riadenie zraniteľnosti, patching a bezpečná konfigurácia;
- penetračné testovanie pre aplikácie;
- webová aplikácia Firewall;
- bezpečné kódovanie;
- údaje sa uchovávajú iba v dátových centrách EÚ a v prípade laptopov sú šifrované na lokálnom zariadení.

E. Zariadenia konečného užívateľa sú chránené

Pracovníci spoločnosti Worldline pracujú s laptopom / desktop na zabezpečenej sieti Worldline. Sú zavedené nasledujúce bezpečnostné opatrenia:

- šifrovanie harddisku na laptopoch pridelených spoločnosťou;
- 2-faktorová autentifikácia (PKI / Alternatíva) pre prácu na diaľku;
- centrálne riadená antivírová ochrana, patching, firewall, HIPS;
- riadenie a monitorovanie softvéru na kontrolu inštalácie neautorizovaného softvéru;
- bezpečné riadenie cyklu životnosti zariadení.

F. Bezpečnosť prístupu na diaľku

2-faktorová autentifikácia sa používa pre prístup na diaľku do kritických cieľových systémov spoločnosti Worldline. Pre systémy riadené spoločnosťou Worldline sa poskytuje riešenie VPN (Virtual Private Network) na pripojenie k sieti Worldline a pre neriadené systémy je dodatočne zavedené riešenie VDI (Virtual Desktop Infrastructure).

Akékoľvek iné zriadenie pripojenia musí byť vopred schválené oddelením bezpečnosti.

G. Kontrola prístupu k Osobným údajom

Pracovníci s prístupom k osobným údajom môžu mať prístup iba k tým údajom, ktoré sú nevyhnutné na vykonávanie činností, za ktoré sú zodpovední. Oprávnenie na prístup sa udeľuje na základe „princípu najnižších privilégií" a zakladá sa buď na role, alebo na mene. Sú zavedené protokoly a revízne záznamy prístupu a je pridelená zodpovednosť za kontrolu prístupu.

H. Bezpečnosť, dôvernosť a dostupnosť osobných údajov

Na základe posúdenia rizík (a ak sa to vyžaduje aj dodatočnej DPIA) spoločnosť Worldline zabezpečí úroveň bezpečnosti primeranú riziku vrátane okrem iného podľa daného prípadu:

- anonymizácie a šifrovania Osobných údajov;
- schopnosti zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracúvania;
- schopnosti obnoviť dostupnosť a včasný prístup k Osobným údajom v prípade fyzického alebo technického incidentu;
- procesu pre pravidelné testovanie, posudzovanie a hodnotenie účinnosti technických a organizačných opatrení na zabezpečenie bezpečnosti spracúvania;
- zabezpečenia logického oddelenia údajov svojich zákazníkov;
- zriadenia procesu na zachovanie aktuálnosti a správnosti spracúvaných údajov;
- vedenia záznamov o činnostiach spracovania podľa nariadenia GDPR;
- opatrení na odhalenie neoprávneného prístupu prostredníctvom systémov na zaznamenávanie prístupu;
- uchovávania údajov o zákazníkoch (vrátane záložných kópií a archívov), iba pokiaľ to bude slúžiť na účely, pre ktoré boli údaje získané, a v súlade s pokynmi zákazníkov, pokiaľ neexistuje zákonná alebo zmluvná povinnosť uchovávať údaje dlhšiu dobu;
- procesu riadenia incidentov a plánov reakcie na incidenty;
- postupu oznamovania porušení ochrany údajov;
- núdzových plánov a plánov obnovy po katastrofe obsahujúcich postupy a priradenie zodpovedností (záložný rezervný plán).