OBCHODNÍ SLUŽBY SPOLEČNOSTI WORLDLINE

Technická a organizační opatření a Seznam Oprávněných subdodavatelů

1. ÚČEL TOHOTO DOKUMENTU

Tento dokument obsahuje seznam technických a organizačních opatření, která platí jako standard. Vlastní přijatá opatření závisí na Službě a místě příslušného zpracování, a to z toho důvodu, že ne všechna opatření jsou relevantní pro všechny Služby a místa. Společnost Worldline zaručuje, že má pro všechny Služby a místa k dispozici nezbytná adekvátní technická a organizační opatření, jež jsou obsažena v níže uvedeném seznamu. Opatření jsou navržena tak, aby:

- zajišťovala bezpečnost a důvěrnost Osobních údajů;
- chránila před jakýmikoli očekávanými hrozbami nebo nebezpečím pro bezpečnost a integritu (celistvost) Osobních údajů;
- chránila před jakýmkoli skutečným neoprávněným zpracováním, ztrátou, používáním, zveřejněním nebo získáním Osobních údajů nebo přístupu k nim.

Společnost Worldline se zavazuje neustále sledovat účinnost svých opatření v oblasti ochrany informací. Společnost Worldline se zavazuje udržovat svůj stav shody se souborem bezpečnostních norem PCI DSS[1].

Tento dokument dále obsahuje seznam subdodavatelů, které společnost Worldline používá pro zabezpečení svých služeb v rámci akceptace platebních karet pro Obchodníky. Tento seznam bude aktualizován (pokud dojde ke změně), a to vždy k prvnímu pracovnímu dni každého čtvrtletí dle Podmínek pro zpracování údajů. Tato aktualizace je považována za oznámení společnosti Worldline Obchodníkovi, jejíž součástí jsou všichni Oprávnění subdodavatelé.

2. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

A. Lidé, povědomí a lidské zdroje:

- Všechny nábory se řídí procesem ověřování (screeningu) podle zásad skupiny Worldline v oblasti ověřování údajů, a sice v mezích místních předpisů;
- V každé smlouvě má každý zaměstnanec zabudována ustanovení Dohody o zachování důvěrnosti informací;
- Všichni zaměstnanci jsou povinni každoročně absolvovat školení v oblasti povědomí o Etickém kodexu, (včetně testu);
- Zaměstnanci společnosti Worldline jsou povinni každoročně absolvovat školení společnosti Worldline v oblasti ochrany údajů, školení o ochraně informací a informační bezpečnosti a bezpečnostní školení v oblasti PCI DSS, včetně testu;
- Všichni zaměstnanci jsou informováni o prohlášení o zásadách v oblasti bezpečnosti a zásadách ochrany údajů;
- Všichni zaměstnanci jsou povinni dodržovat platné předpisy společnosti Atos a skupiny Worldline v oblasti zabezpečení a ochrany údajů, jakož i místní předpisy v této oblasti;
- Pravidelná komunikace se všemi zaměstnanci za účelem zajištění informovanosti o Obecném nařízení o ochraně osobních údajů (GDPR), (vedle školení o zásadách společnosti Worldline v oblasti ochrany údajů a školení v oblasti ochrany informací a informační bezpečnosti);
- Další specifická školení zajišťovaná orgány pro ochranu údajů za účelem výběru týmů a zaměstnanců.

[1] PCI DSS: Payment Card Industry – Data Security Standard = Odvětví platebních karet – Standard bezpečnosti dat - týkající se ochrany údajů o držiteli karet.

B. Organizační řízení

Společnost Worldline bude udržovat svou vnitřní organizaci způsobem, který splňuje požadavky platné legislativy a požadavky Správce údajů na zabezpečení údajů. To se uskuteční:

- prostřednictvím úředníka (referenta) pro ochranu osobních údajů;
- zavedením organizace a správy pro ochranu osobních údajů, jejich zabezpečení a pro zajištění kontinuity provozu;
- rozsáhlou sítí odborníků společností Atos a Worldline v oblasti ochrany údajů;
- stanovením úloh a odpovědností vztahující se k ochraně osobních údajů pro všechny pracovníky;
- pomocí souboru zásad, které upravují ochranu a bezpečnost údajů;
- pomocí interních zásad, postupů a procesů v oblasti zpracování údajů pro kódování, testování, změny a vydávání aktuálních verzí, pokud se budou vztahovat na zpracovávané Osobní údaje;
- realizací kontrolního rámce ochrany údajů, jehož soulad bude pravidelně posuzován;
- Provádějí se pravidelné interní bezpečnostní audity za účelem ověření bezpečnostních postupů;
- Zajištění stejných technických a organizačních opatření platí pro dodavatele, kteří zpracovávají osobní údaje.

C. Fyzická ochrana a bezpečnost a papírové záznamy:

Všechny subjekty ve skupině dodržují zásady fyzické a environmentální bezpečnosti a standard ochrany informací:

- řízení fyzického přístupu je realizováno u všech zaměstnanců, a systémy řízení návštěv jsou realizovány u všech návštěvníků/hostů;
- kontroly fyzického přístupu jsou prováděny v definovaných cyklech;
- informace, které zahrnují papírové dokumenty, jsou klasifikovány, označovány, chráněny a zpracovávány podle interního předpisu společnosti Worldline týkajícího se klasifikace informací;
- specifická pravidla určují, jak ukládat, zpracovávat, zobrazovat, tisknout, přenášet a ničit záznamy (jak v elektronické, tak v papírové podobě);
- střežení pomocí kamerového systému (CCTV) k ochraně vyhrazených prostor;
- protipožární ochrana, protipovodňová ochrana, systémy vytápění, klimatizace a zálohovací systémy napájení jsou nainstalovány pro zajištění integrity a dostupnosti dat uložených v datových centrech;
- řízená likvidace datových médií.

D. Zabezpečení technické infrastruktury a aplikací:

Společnost Worldline realizovala bezpečnostní prostředí s ochranou do hloubky, které zajišťuje několik úrovní zabezpečení. Jsou zahrnuta následující bezpečnostní opatření:

- oddělení a segmentace sítí;
- zabezpečený přenos údajů přes nedůvěryhodné sítě;
- osobní údaje uložené v produkčních sítích, které jsou odděleny pomocí firewallů;
- systémy IDS (Intrusion Detection – detekce narušení) a IPS (Intrusion Prevention – prevence narušení) – a monitorování (SIEM – Security Information and Event Management System = Správa bezpečnostních informací a událostí);
- bezpečnostní brány a řešení VPN (virtuální privátní sítě) pro vzdálené připojení;
- správa zranitelnosti, patching (záplatování) a zabezpečená konfigurace;
- penetrační testování aplikací;
- webová aplikace Firewall;
- bezpečné kódování;
- Údaje jsou uloženy pouze v datových centrech EU a v případě notebooků jsou zašifrovány na místním zařízení.

E. Zařízení koncových uživatelů jsou chráněna

Zaměstnanci společnosti Worldline pracují s notebookem nebo počítačem na zabezpečené síti společnosti Worldline. Jsou zahrnuta následující bezpečnostní opatření:

- šifrování pevného disku na noteboocích přidělených společností;
- dvoufaktorová autentizace (PKI – Public Key Infrastructure = Infrastruktura veřejných klíčů / alternativní) pro práci na dálku;
- centrálně řízená antivirová ochrana, patching (záplatování), firewall, systém prevence narušení hostitele;
- správa a sledování softwaru pro kontrolu instalace neoprávněného softwaru;
- zabezpečení životního cyklu zařízení.

F. Zabezpečení vzdáleného přístupu

Používá se dvoufaktorová autentizace pro vzdálený přístup ke kritickým cílovým systémům společnosti Worldline. Pro systémy řízené společností Worldline je k dispozici řešení VPN (virtuální privátní síť) pro připojení k síti Worldline, a pro nespravované systémy navíc existuje řešení VDI (Virtual Desktop Infrastructure = virtuální desktopová infrastruktura).

Jakékoliv další nastavení připojení musí být předem schváleno bezpečnostním oddělením.

G. Řízení přístupu k osobním údajům

Zaměstnanci s přístupem k osobním údajům mají přístup pouze k údajům, které jsou nezbytné pro účely činností, za něž odpovídají. Přístupové oprávnění je udělováno na základě zásady „nejnižšího oprávnění“ a vychází z funkce nebo jména (zaměstnance). Přístupové protokoly a kontrolní cesty jsou nainstalovány, a je přiřazena odpovědnost za řízení přístupu.

H. Zabezpečení, důvěrnost a dostupnost osobních údajů

Na základě posouzení rizik (a pokud to bude požadováno, na základě dalšího posouzení vlivu na ochranu osobních údajů - DPIA) společnost Worldline zajistí úroveň zabezpečení odpovídající riziku, což bude mimo jiné případně zahrnovat:

- anonymizaci a šifrování Osobních údajů;
- schopnost zajistit trvalé zachování důvěrnosti, integrity, dostupnosti a odolnosti zpracovatelských systémů a služeb;
- schopnost včas obnovit dostupnost Osobních údajů a přístup k nim v případě bezpečnostního incidentu fyzické či technické povahy;
- postup pro pravidelné testování, posuzování a hodnocení účinnosti technických a organizačních opatření pro zajištění bezpečnosti zpracování;
- zajištění logického oddělení jejích zákaznických údajů;
- nastavení procesu, který zajistí přesnost a aktuálnost zpracovávaných údajů;
- uchování záznamů o zpracovatelských činnostech podle Obecného nařízení o ochraně osobních údajů (GDPR);
- opatření pro zjištění neoprávněného přístupu prostřednictvím systémů protokolování přístupu;
- Údaje o zákaznících (včetně záloh a archivů) budou uchovávány pouze po dobu, během níž budou sloužit účelům, pro které byly shromážděny podle pokynů zákazníků, pokud nebude existovat zákonná nebo smluvní povinnost uchovávat tyto údaje po delší časové období;
- proces správy incidentů a plány reakce na incidenty;
- postup oznamování porušení zabezpečení údajů;
- Havarijní plány a plány na obnovu po havárii s postupy a přidělením odpovědností (záložní plány pro případ nouze) jsou vypracovány.

3. SEZNAM OPRÁVNĚNÝCH SUBDODAVATELŮ

A. Členové skupiny Atos

Název	Sídlo
Worldline SA	- Z.I.A., Rue de la Pointe, F-59113 Seclin, France - 19, Rue de vallée Maillard, BP 1311, F-41013 Blois Cedex, France - 38, route d'Azé, CS 40095, 14102 Vendôme Cedex, France - 53, Ave Paul Kruger, CS 60195 Villeurbanne Cedex, France
equensWorldline SE, Belgian Branch	- Haachtsesteenweg 1442, 1130 Brussels, Belgium
equensWorldline SE, France Branch	- 80 Quai Voltaire, Immeuble River Ouest, 985870 Bezons, France

B. Oprávnění subdodavatelé – třetí strany Third Party Sub Contractors

Název	Sídlo
Energize Global Services	- 6/1 Abelian St, IT Park Building, Yerevan 0038, Armenia
Komerční banka, a.s.	- Na Příkopě 33 / 969, 114 07 Prague 1
SONET, společnost s.r.o.	- Lužická 2093/9, 616 00 Brno
Global Payments Europe, s.r.o.	- V Olšinách 625/80,100 00 Záběhlice