Technická a organizační opatření Worldline Financial Services (Europe) S.A.

(EU CZ)

1 Účel tohoto dokumentu

Tento dokument obsahuje seznam technických a provozních opatření, která jsou standardně použitelná. Konkrétní přijatá opatření závisí na dané službě a místě zpracování 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 odpovídající technická a provozní opatření uvedená v níže uvedeném seznamu po posouzení vlivu na ochranu osobních údajů. Cílem opatření je:

- Zajistit bezpečnost a důvěrnost osobních údajů.
- Chránit před jakýmikoliv předpokládanými hrozbami nebo nebezpečími pro bezpečnost a integritu osobních údajů.
- Chránit před jakýmkoli neoprávněným zpracováním, ztrátou, použitím, zveřejněním nebo získáním jakýchkoli osobních údajů nebo přístupem k nim.

Stránka obsahuje také seznam subdodavatelů, které společnost Worldline využívá k poskytování svých služeb. Společnost Worldline zajišťuje, aby všichni její dílčí zpracovatelé poskytli odpovídající záruky ochrany osobních údajů, které zpracovávají naším jménem, a to prostřednictvím kontroly subdodavatelů: nemělo by docházet k žádnému pověřenému zpracování údajů ve smyslu čl. 28 nařízení GDPR bez příslušných pokynů zadavatele, např. jasného návrhu smlouvy, formalizované správy subdodávek a přísného výběru zpracovatelů (certifikace ISO, ISMS), předchozího prokázání způsobilosti, následného monitorování.
Společnost Worldline se zavazuje k průběžnému sledování účinnosti svých opatření na ochranu údajů a ke každoročnímu auditu shody prováděnému třetí stranou, aby se ujistila o zavedených opatřeních a kontrolách.

2 Technická a organizační opatření

A Lidé, informovanost a lidské zdroje:

- Při všech náborech probíhá prověřování podle principů zásad prověřování společnosti Worldline.
- Součástí každé smlouvy se zaměstnancem jsou i ustanovení o mlčenlivosti.
- Školení informovanosti o etickém kodexu (včetně testu) je každoroční povinností pro všechny zaměstnance a provádí se prostřednictvím speciálního e-learningového modulu.
- Zásady přijatelného používání IT skupiny nebo jejich místní verze jsou sdíleny se všemi zaměstnanci.
- Prohlášení o zásadách bezpečnosti podepsané managementem je sdíleno se všemi zaměstnanci.
- Zaměstnanci společnosti Worldline jsou povinni každoročně absolvovat školení o zásadách ochrany osobních údajů, zabezpečení informací a bezpečnosti (včetně testu) společnosti Worldline.
- Pravidelná školení informovanosti o GDPR pro všechny zaměstnance (kromě školení o zásadách ochrany osobních údajů, zabezpečení informací a bezpečnosti společnosti Worldline);
- Přístup k systémům je poskytován na základě „nezbytné potřeby" s ohledem na rozdělení povinností.
- Pravidelně se provádějí interní bezpečnostní audity za účelem ověření bezpečnostních postupů.

B Fyzická bezpečnost a papírové záznamy:

Dodržování zásad fyzické a environmentální bezpečnosti skupiny Worldline:

- Zavedení systémů kontroly přístupu a řízení návštěv týkající se všech návštěvníků/hostů.
- Fyzická kontrola přístupu (ochrana proti neoprávněnému přístupu k zařízením pro zpracování nebo ukládání údajů): zejména s využitím magnetických nebo čipových karet, elektrických zařízení pro otevírání dveří, vrátného, pracovníků ostrahy, poplašných systémů, kamerových systémů.
- Kontroly fyzického přístupu podle stanoveného harmonogramu.
- Čistý stůl, čistá obrazovka a zabezpečený tisk, implementovaný proces.
- Informace, včetně papírových dokumentů, se kterými dovozce údajů nakládá, jsou klasifikovány, označeny, chráněny a je s nimi nakládáno v souladu s pravidly klasifikace informací společnosti Worldline.
- S výjimkou předchozího zvláštního svolení se stolní počítače z pracoviště neodstraňují.
- Kamerový systém na ochranu prostor s omezeným přístupem.
- Zavedení požárního poplachu a protipožárních systémů pro bezpečnost zaměstnanců.
- Požární evakuační cvičení se konají ve stanovených harmonogramech.

C Vzdálené koncové zařízení uživatele je chráněno:

Uživatelé pracují na dálku s notebooky a stolními počítači v zabezpečené síti skupiny Worldline, kterou pro skupinu Worldline spravuje společnost Global IT. Kromě toho jsou zavedena i tato bezpečnostní opatření:

- Šifrování pevného disku v noteboocích přidělených společností.
- Dvoufaktorové ověřování (PKI/alternativní).
- Centrálně spravovaná a antivirová ochrana.
- Správa a monitorování softwaru pro kontrolu instalace schváleného softwaru.
- Pro přístup k informacím je zavedena kontrola pomocí přihlašovacího ID a hesla.
- Provádí se pravidelná kontrola přístupu.
- E-maily jsou automaticky kontrolovány antivirovým a antispamovým softwarem.

D Zabezpečení vzdáleného přístupu

Pro vzdálený přístup ke klíčovým cílovým systémům skupiny Worldline se obecně používá dvoufaktorové ověřování. Pokud je zdrojem vzdáleného připojení systém řízený společností Worldline, je provedeno ověření zařízení na základě certifikátu v zařízení.
Jakékoli jiné nastavení připojení musí být předem schváleno bezpečnostním oddělením.

E Obecná bezpečnostní opatření jsou mj.:

- Údaje jsou uloženy v datových centrech v EU a ve Švýcarsku nebo v případě přenosných počítačů šifrovaně v místním zařízení.
- Ukončení připojení přístupu v demilitarizované zóně.
- Veškeré připojení až do zabezpečené oblasti (zóna PCI) je šifrované.
- Přístup do zóny PCI je možný pouze pomocí silného ověření prostřednictvím poskytnutého bezpečnostního klienta.
- Je třeba projít několika vrstvami firewallů a detekce narušení.
- Řízení přístupu podle principů řízení přístupu na základě rolí.
- Řízení ochrany osobních údajů, včetně pravidelného školení zaměstnanců.
- Řízení reakce na incidenty.
- Výchozí nastavení podporující ochranu osobních údajů.

F Kontrola přístupu k osobním údajům

Zaměstnanci s přístupem k soukromým údajům mohou přistupovat pouze k údajům, které jsou nezbytné pro účely činností, za něž jsou odpovědní. Oprávnění přístupu je poskytováno na základě „potřeby vědět" a „potřeby přístupu" a závisí buď na rolích, nebo na jménech. Jsou nastaveny protokoly přístupu a je přidělena odpovědnost za kontrolu přístupu.

Jsou zavedena tato opatření:

- Povinnost zaměstnanců dodržovat platné zásady skupiny Worldline a místní bezpečnostní zásady a zásady ochrany osobních údajů.
- Pracovní pokyny pro nakládání se soukromými údaji.
- Elektronická kontrola přístupu (ochrana proti neoprávněnému použití systémů pro zpracování nebo ukládání údajů): zejména prostřednictvím hesel (včetně odpovídajících zásad), automatických mechanismů blokování, dvoufaktorového ověřování, šifrování datových nosičů.
- Interní kontrola přístupu (prevence neoprávněného čtení, kopírování, úpravy nebo odstranění údajů v rámci společnosti Worldline): zejména pomocí profilů standardního oprávnění na základě zásady „potřeby vědět", standardního procesu přidělování uživatelských práv, zaznamenávání přístupu, pravidelné kontroly přidělených práv, zejména účtů správců.
- Řízená skartace datových médií.
- Jsou zavedeny postupy pro kontrolu dodržování postupů a pracovních pokynů.

G Bezpečnost a důvěrnost osobních údajů

Na základě posouzení rizik (a v případě potřeby dalšího posouzení vlivu na ochranu osobních údajů) zajistí společnost Worldline úroveň zabezpečení odpovídající riziku, mimo jiné prostřednictvím:

- Schématu klasifikace údajů: kategorizace osobních údajů podle stupně důvěrnosti na základě zákonných povinností nebo vlastního posouzení.
- Zákazu neoprávněného čtení, kopírování, úpravy nebo odstranění během elektronického přenosu nebo předávání: zejména prostřednictvím šifrování a virtuálních privátních sítí (VPN).

110.0788.08 EU_CZ/04.2022

- Schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování.
- Ochrany proti náhodnému nebo úmyslnému zničení či ztrátě, jako je strategie zálohování (online/offline; na pracovišti/mimo něj), nepřerušitelný zdroj napájení (UPS, dieselový generátor), antivirový program, firewall, výstražné kanály a plány pro případ nouzové situace; bezpečnostní kontroly na úrovni infrastruktury a aplikací, víceúrovňový plán zabezpečení s outsourcingem zálohování v centrech pro zálohování dat, standardní procesy v případě změny/odchodu zaměstnanců;
- Schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- Procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování (interní audit, PCI-DSS, ISO 27001, národní dozorové orgány).
- Zpracování registrů podle požadavků nařízení GDPR
- Používání systémů protokolů přístupu pro relevantními účely, aby bylo možné odhalit pokusy o neoprávněný přístup
- Hlavní údaje a metadata zákazníků (včetně záloh, archivů, souborů protokolů atd.) budou uchovávány pouze po dobu, po kterou slouží účelům, pro které byly údaje shromážděny, pokud neexistuje zákonná nebo smluvní povinnost uchovávat údaje po dobu delší.

H Organizační kontrola

Zpracovatel údajů bude svou vnitřní organizaci udržovat tak, aby splňovala požadavky platných právních předpisů a požadavky správce údajů na zabezpečení údajů. Tohoto se dosáhne:

Interními zásadami a postupy zpracování údajů, směrnicemi, pracovními pokyny, popisy procesů a předpisy pro programování, testování a vydávání v míře, v jaké se týkají osobních údajů předávaných správcem;

Zavedením rámce kontrol ochrany údajů, jehož dodržování je každoročně přezkoumáváno;

Nastavením plánu pro případ nouzové situace s postupy a rozdělením odpovědností (záložní pohotovostní plán).