Műszaki és szervezeti intézkedések Worldline Financial Services (Europe) S.A.

(EU HU)

1 A dokumentum célja

Ez a dokumentum azokat a műszaki és működéssel kapcsolatos intézkedéseket sorolja fel, amelyeket alap esetben alkalmazni lehet. Az adott időpontban végrehajtandó intézkedések a Szolgáltatótól és a felhasználás helyétől, mivel nem minden intézkedés vonatkozik minden Szolgáltatóra és minden helyszínre. A Worldline garanciát vállal arra, hogy minden Szolgáltató és helyszín esetén fennálljanak a szükséges, megfelelő műszaki és működéssel kapcsolatos intézkedések a lenti felsorolás szerint, az Adatvédelmi Hatás Kiértékelése (Data Protection Impact Assessment) alapján. Az intézkedéseket úgy tervezték, hogy:

- biztosítsák a Személyes adatok biztonságát és titkosságát;
- védelmet adjanak bármely várható, a Személyes adatok biztonságával és integritásával kapcsolatos fenyegetéssel vagy kockázattal szemben;
- védelmet adjanak bármely Személyes adat bármely aktuális, engedély nélküli feldolgozása, elvesztése, használata, közzététele vagy megszerzése, illetve az ezekhez való hozzáférés ellen.

Az oldalon megtalálja a Worldline szolgáltató alvállalkozóinak a listáját. A Worldline az alvállalkozói ellenőrzésével biztosítja, hogy minden alvállalkozója megfelelő garanciát nyújtson a nevében az alvállalkozó által feldolgozott személyes adatok védelmére: nem történhet semmilyen adatfeldolgozási megbízás a GDPR 28. cikkelye értelmében a fővállalkozó megfelelő utasításai nélkül, mint amilyen pl. a világosan megfogalmazott szerződés, a szerződésben rögzített alvállalkozói ügyvitel és az adatfeldolgozó alvállalkozók szigorú kiválasztása (ISO minősítés, ISMS), az előzetes alkalmassági vizsgálat és a folyamatos nyomon követés.
A Worldline vállalja, hogy folyamatosan nyomon követi az általa adott információk védelmének hatékonyságát, és évente elvégeztet egy auditot egy külső céggel az intézkedések minőségének biztosítása, és a helyszíni ellenőrzések elvégzése érdekében.

2 Műszaki és szervezeti intézkedések

A Emberek, tudatosság és HR:

- Minden személyzeti felvételi eljárás a Worldline háttérellenőrző politikája alapelveinek megfelelő átvilágítási folyamatot követ;
- Minden alkalmazott minden szerződése tartalmaz egy Titoktartási megállapodás záradékot;
- Az Etikai kódex tudatos alkalmazása tréninget (amely egy tesztet is tartalmaz) minden alkalmazottnak évente kötelezően el kell végeznie egy személyre szabott e-learning modulon keresztül;
- Az IT Csoport Elfogadható használat politikájáról vagy annak helyi változatáról minden alkalmazott tájékoztatást kap;
- A vezetőség által aláírt Biztonsági politika nyilatkozatot minden alkalmazott megkapja;
- A Worldline munkavállalói kötelesek évente elvégezni egy Információ-biztonsági tréninget (amely egy tesztet is tartalmaz), a Worldline adatvédelmi politikájával összhangban;
- Rendszeres GDPR tudatossági tréningek minden alkalmazott számára (a Worldline adatvédelmi politikán és az Információ-biztonság tréningen túlmenően);
- A rendszerekhez való hozzáférés igény szerinti alapon biztosított, figyelembe véve a feladatok elkülönítését;
- Rendszeres belső biztonsági auditok a biztonsági eljárások gyakorlatának ellenőrzésére.

B Fizikai biztonság és papír alapú naplózás:

A Worldline csoport Fizikai és környezeti biztonság politikájának teljesítése:

- Hozzáférés-ellenőrzés és látogató-kezelő rendszerek alkalmazása minden látogató/vendég esetében;
- Fizikai hozzáférés ellenőrzése (védelem az engedély nélküli adatfeldolgozás vagy raktározás ellen): különösen mágneskártyákkal vagy okoskártyákkal, elektromos ajtónyitókkal, portással, biztonsági alkalmazottakkal, riasztó rendszerekkel, videó rendszerekkel.
- A fizikai hozzáférések felülvizsgálata előre meghatározott rendszerességgel;
- Tiszta asztal, tiszta képernyő és nyomtatáskövető eljárás alkalmazása;
- A tájékoztatás, amibe bele tartoznak a papír alapú dokumentumok, amelyeket az adat-bevivő kezel, a Wordline információ-osztályozási politikának megfelelően vannak osztályozva, címkézve, védve és kezelve;
- Az asztal anyagait nem lehet elvinni a helyükről, kivéve az arra vonatkozó előzetes engedéllyel;
- CCTV felügyelet a korlátozott belépéssel védett területek védelmére;
- Tűzriasztás és tűzvédelmi rendszerek az alkalmazottak biztonságának védelmére;
- Tűzvédelmi kiürítési gyakorlatok meghatározott rendszerességgel;

C A távoli végfelhasználói eszközök védelme:

A távoli felhasználók a laptopon és az asztali számítógépen egy Worldline által biztosított hálózaton dolgoznak, amelyet a Global IT tart fenn a Worldline csoport számára. A következő biztonsági intézkedések vannak ezen felül beépítve:

- A vállalati laptopok merevlemezeinek kódolása;
- Kétlépcsős azonosítás (PKI/Alternatív);
- Központilag kezelt vírusvédelem;
- A szoftver kezelése és monitorozása egy engedélyezett szoftver telepítés ellenőrzéséhez;
- Belépési azonosító és jelszó ellenőrzés az információhoz való hozzáféréshez;
- Rendszeres hozzáférés felülvizsgálata;
- Az e-maileket automatikusan ellenőrzik vírusvédelmi és spamszűrő szoftverek.

D Távoli hozzáférés biztonsága

Általában kétlépcsős azonosítást alkalmazunk a kritikus Wordline célrendszerekhez való távoli hozzáférés esetében. Ha a távoli kapcsolat forrása egy Worldline által ellenőrzött rendszer, az eszközön lévő igazoláson alapuló eszköz autentikációt használunk.
Minden más kapcsolatot előre engedélyeztetni kell a biztonsági osztállyal.

E Az általános biztonsági intézkedések a következők:

- Az adatokat az EU és CH Adattároló Központjaiban tárolják, vagy laptopok esetén a kódolt helyi eszközön;
- A hozzáférési kapcsolat lezárása a Demilitarizált zónában;
- A biztosított területig (PCI zóna) minden kapcsolódási lehetőség kódolva van;
- A PCI zónához való hozzáférés csak erős autentikációval lehetséges megadott biztonsági klienssel;
- Többszintű tűzfal és behatolás-védelmen keresztül kell átjutni;
- A hozzáférést a Szerep alapú hozzáférés-ellenőrzés (RBAC) alapelveinek megfelelően kezeljük.
- Az adatvédelem magában foglalja az alkalmazottak rendszeres képzését;
- Incidensválasz-kezelés;
- Adatvédelem-barát alapértelmezett beállítások;

F A Személyes adatokhoz való hozzáférés ellenőrzése

A személyes adatokhoz hozzáféréssel rendelkező alkalmazottak csak azokhoz az adatokhoz férhetnek hozzá, amelyek szükségesek a felelősségi körükbe tartozó feladatok elvégzéséhez. A hozzáférés engedélyezése tudás igény és hozzáférés igény alapon történik, akár szerep szerint akár név alapján. A hozzáférési logok lokálisak, és a hozzáférés ellenőrzésének felelőssége kijelölt feladat.

A következő intézkedéseket foganatosítottuk:

- Az alkalmazottak kötelesek betartani a vonatkozó Worldline politikát és a helyi biztonsági és adatvédelmi politikákat;
- A személyes adatok kezelésére vonatkozó munkahelyi utasítások;
- Elektronikus hozzáférés-ellenőrzés (védelem az adatkezelési vagy adattárolási rendszerek engedély nélküli használata ellen): különösen jelszavakkal (ideértve a vonatkozó politikát is), automata záró mechanizmusokkal, kétlépcsős azonosítással, az adatátvitel kódolásával;
- Belső hozzáférés ellenőrzés (az adatok engedély nélküli elolvasásának, másolásának, módosításának vagy törlésének megelőzése a Worldline-en belül): pontosabban, standard engedélyezési profilok használatával szükséges tudás alapon, standard eljárás a felhasználói jogok, a hozzáférési logok megadására, a megadott jogok rendszeres felülvizsgálata, különösen az adminisztrátori számlák esetében;
- Az adathordozók ellenőrzött megsemmisítése;
- Az eljárások és munkahelyi utasítások teljesítésére vonatkozó ellenőrzési eljárások helyben kerülnek meghatározásra;

110.0788.06 EU_HU/04.2022

G A személyes adatok biztonsága és titkossága

Kockázati felmérés alapján (és ha további DPIA szükséges) a Worldline a kockázatnak megfelelő biztonsági szintet biztosít, ideértve, többek között, mint megfelelő eszközöket:

- Az adatok osztályozási táblázata: a személyes adatok besorolása azok titkossági szintje szerint a törvényi kötelezettségek vagy önértékelés alapján.
- Az adatok nem olvashatók el, nem másolhatók le, nem módosíthatók és nem törölhetők engedély nélkül azok elektronikus átadása vagy átvitele során: különösen kódolással és a Virtuális Privát Hálózatokon (VPN) keresztül;
- Képesek vagyunk biztosítani az adatfeldolgozó rendszerek és szolgáltatások mindenkori titkosságát, integritását, elérhetőségét és rugalmasságát;
- Védelem az adatok véletlen vagy szándékos megsemmisítése vagy elvesztése ellen, mint amilyen a háttértár-stratégia (online/offline; on-site/off-site), a szünetmentes áramforrás (UPS, dízel generátor szett), vírusvédelem, tűzfal, figyelmeztető csatornák és vészhelyzeti tervek; biztonsági ellenőrzések az infrastruktúra és az alkalmazási szintek tekintetében, többszintű biztonsági terv a háttértárak adattároló központokba kihelyezésével, standard eljárások az alkalmazottak lecserélése/elbocsátása esetén;
- Képesek vagyunk visszaállítani a Személyes adatok elérhetőségét és hozzáférhetőségét kellő időn belül, ha fizikai vagy technikai jellegű incidens következik be;
- A műszaki és szervezeti intézkedések hatékonyságának rendszeres tesztelési, felmérési és kiértékelési eljárása az adatfeldolgozás biztonságának biztosítása érdekében (belső audit, PCI-DSS, ISO27001, nemzeti ellenőrző intézmények).
- Az eljárások naplózása a GDPR követelményeinek megfelelően.
- A log-rendszerek használatához való hozzáférés megfelelő módon ahhoz, hogy megállapíthassuk az engedély nélküli próbálkozásokat.
- A fő ügyfél-adatok és meta adatok esetén (ideértve a háttértárakat, archívumokat, log-fájlokat, etc.) csak addig lesznek tárolva, ameddig az szükséges abból a célból, amelyért az adatok begyűjtésre kerültek, kivéve, ha törvényi vagy szerződéses kötelezettség előírja azok hosszabb ideig tartó megőrzését.

H Szervezeti ellenőrzés

Az Adatfeldolgozónak fenn kell tartania belső szervezetét olyan módon, hogy az megfeleljen a vonatkozó törvényi előírásoknak és az Adatkezelő adatbiztonsági követelményeinek. Ennek meg kell felelniük: a belső adatfeldolgozási politikáknak és eljárásoknak, utasításoknak, munkaköri utasításoknak, eljárás leírásoknak és programozási, tesztelési és törlési szabályozásoknak, amennyiben ezek az Adatkezelő által átadott Személyes adatokra vonatkoznak;

Egy Adatvédelmi ellenőrzési keretszabályozás alkalmazása, aminek a teljesítését éves szinten auditálják;

Egy vészforgatókönyv alkalmazása a helyi eljárások és felelősök kijelölésével (háttértár-incidens terv).