Tehničke i organizacijske mjere
Worldline Financial Services (Europe) S.A.

(EU HR)

1 Svrha ovog dokumenta

Ovaj dokument sadrži popis tehničkih i operativnih mjera koje u primjeni služe kao standard. Već poduzete mjere ovise o Usluzi i mjestu dotične obrade iz razloga što nisu sve mjere relevantne za sve Usluge i sve lokacije. Worldline jamči da za sve Usluge i lokacije ima potrebne odgovarajuće tehničke i operativne mjere, koje su uključene u donji popis ispod Procjene učinka zaštite podataka. Mjere su namijenjene:

- osiguravanju sigurnost i povjerljivost osobnih podataka;
- zaštititi od svih očekivanih prijetnji ili opasnosti po sigurnost i integritet osobnih podataka;
- zaštititi od stvarne neovlaštene obrade, gubitka, upotrebe, otkrivanja ili stjecanja ili pristupa bilo kojim Osobnim podacima

Na ovoj stranici se također nalazi popis podizvođača koje Worldline koristi za pružanje svojih usluga. Worldline omogućuje da svi njezini pod-procesori pružaju odgovarajuća jamstva za zaštitu osobnih podataka koje obrađuju u naše ime, na temelju kontrola podugovarača: obrada podataka se ne bi smjela naručivati kod trećih osoba u smislu čl. 28 Opće uredba o zaštiti osobnih podataka, ukoliko ne postoje odgovarajuće upute glavnog naručitelja, npr. jasan okvir ugovora, formalizirano upravljanje podugovaranjem i strog odabir procesora (ISO-certifikacija, ISMS), prethodno dokazivanje sposobnosti, nadzor radi praćenja.
Worldline se obvezuje na kontinuirano praćenje učinkovitosti svojih informacijskih zaštitnih mehanizama i na godišnju reviziju usklađenosti koju obavlja treća strana, a sve u cilju pružanja jamstva o provedenim mjerama i kontrolama.

2 Tehničke i organizacijske mjere

A Osoblje, informiranost i ljudski potencijali:

- Pri zapošljavanju, za svako radno mjesto vrši se postupak provjere u skladu s načelima politike Worldline o provjeri osnovnih informacija;
- U svakom ugovoru svakog zaposlenika nalazi se odredbe o neobjelodanjivanju podataka;
- Obuka o informiranosti o etičkom kodeksu (uključujući i test) godišnja je obveza svih zaposlenika i provodi se kroz namjenski modul za e-učenje;
- Svi zaposlenici dobivaju pravila grupe o prihvatljivoj uporabi informatičke tehnologije ili lokalnu verziju tih pravila;
- Svi zaposlenici dobivaju izjavu o sigurnosnoj politici koju je potpisala Uprava;
- Osoblje tvrtke Worldline mora svake godine pohađati obuku o Worldline politici zaštite podataka te obuku o informacijskoj zaštiti i sigurnosti (uključujući i test);
- Redoviti treninzi informiranosti o Općoj uredbi o zaštiti osobnih podataka (GDPR) za sve zaposlenike (uz Worldline politiku zaštite podataka te obuku o informacijskoj zaštiti i sigurnosti);
- Pristup sustavima pruža se na temelju „potrebe", uzimajući u obzir razdvajanje dužnosti;
- Provode se redovite unutarnje revizije sigurnosti i zaštite radi provjere sigurnosnih praksi.

B Fizička sigurnost i papirnata evidencija:

Usklađenost sa politikom Grupe o Worldline fizičkoj i okolišnoj sigurnosti:

- Sustavi kontrole pristupa i upravljanja posjetiteljima primjenjuju se na sve posjetitelje/goste;
- Fizička kontrola pristupa (zaštita od neovlaštenog pristupa obradi podataka ili pohrani): posebno pomoću magnetskih ili pametnih kartica, električnih otvarača vrata, vratara, zaštitarskog osoblja, alarmnih sustava, video sustava;
- Pregledi fizičkog pristupa u određenim periodima;
- Proveden postupak čiste računalne radne površine (desktopa), jasno vidljivog zaslona i FollowMe ispisa (ispis preko svakog priključenog aparata);
- Podaci, koji uključuju papirnate dokumente kojima rukuje uvoznik podataka, tj. osoba koja ih unosi, klasificirani su, označeni, zaštićeni i njima se rukuje u skladu s Worldline politikom klasifikacije informacija;
- Stolna računala se ne odnose s lokacije bez prethodnog posebnog odobrenja;
- CCTV nadzor radi zaštite područja sa zabranom pristupa;
- U cilju zaštite zaposlenika postavljeni su protupožarni alarmni i protupožarni sustavi;
- Vježbe za evakuaciju požara provode se na određenim frekvencijama.

C Zaštićeni su uređaji udaljenog krajnjeg korisnika:

Udaljeni korisnici rade s prijenosnim i stolnim računalima na Worldline zaštićenoj mreži koju održava Global IT za Worldline Group. Uz to su ugrađene sljedeće sigurnosne mjere:

- Šifriranje hard diska na prijenosnim računalima koja je dodijelila tvrtka;
- Autentifikacija s 2 elementa (PKI/alternativa);
- Središnje upravljanje i antivirusna zaštita;
- Upravljanje i nadzor softvera za kontrolu ovlaštene instalacije softvera;
- Za pristup informacijama primijenjene su kontrole za prijavu i zaporku;
- Provodi se periodični pregled pristupa;
- E-poruke automatski kontrolira antivirusni softver i softver protiv neželjene pošte.

D Sigurnost pristupa na daljinu

Dvodijelna provjera autentičnosti koristi se općenito za pristup na daljinu kritičnim ciljnim Worldline sustavima. Ako udaljena veza potječe iz sustava pod kontrolom Worldline, tada se provodi provjera autentičnosti uređaja na temelju certifikata na uređaju.
Svako drugo postavljanje veza mora prethodno dobiti odobrenje odjela za sigurnost.

E Opće sigurnosne mjere su, među ostalima:

- Podaci se pohranjuju u EU i švicarskim podatkovnim centrima ili u slučaju prijenosnih računala podaci su šifrirani i pohranjeni na lokalnom uređaju;
- Prekid pristupne veze u demilitariziranoj zoni;
- Svako povezivanje sve do sigurne zone (PCI zona) šifrirano je;
- Pristup PCI zoni moguć je samo preko stroge provjere autentičnosti preko dobivenog sigurnosnog klijenta;
- Potrebno je proći više slojeva vatrozidova i otkrivanja upada;
- Pristupom se upravlja prema načelima kontrole pristupa koji se temelje na različitim ulogama;
- Upravljanje privatnošću, uključujući redovitu obuku zaposlenika;
- Upravljanje odgovorima na incidente;
- Standardne postavke prilagođene privatnosti.

F Kontrola pristupa osobnim podacima

Zaposlenici s pristupom privatnim podacima mogu pristupiti samo podacima potrebnim za aktivnosti pod njihovom odgovornošću. Odobrenje pristupa pruža se na temelju načela „potrebno je znati" i „potrebnog pristupa" te na ulozi ili imenu. Zapisnici pristupa su uspostavljeni i dodijeljena je odgovornost za kontrolu pristupa.

Postavljene su sljedeće mjere:

- Obveza zaposlenika da se pridržavaju važećih Worldline i lokalnih sigurnosnih politika te politika zaštite podataka;
- Radne upute za rukovanje privatnim podacima;
- Elektronička kontrola pristupa (zaštita od neovlaštene upotrebe sustava za obradu ili pohranu podataka): posebno putem zaporki (uključujući odgovarajuću politiku), mehanizama automatskog zaključavanja, dvodijelne autentifikacije, šifriranja nosača podataka;
- Unutarnja kontrola pristupa (sprječavanje neovlaštenog čitanja, preslikavanja, izmjene ili uklanjanja podataka unutar Worldline-a): naime, korištenjem profila standardne autorizacije na osnovi načela „potrebno je znati", standardnog postupka za dodjelu korisničkih prava, evidentiranja pristupa, periodičnog pregleda dodijeljenih prava, posebno za administratorske račune;
- Kontrolirano uništavanje podatkovnih medija;
- Postavljeni su postupci za provjeru pridržavanja postupaka i radnih uputa.

G Sigurnost i povjerljivost osobnih podataka

Na temelju procjene rizika (i ako je potreban dodatni DPIA), Worldline osigurat će razinu sigurnosti koja odgovara riziku, uključujući, među ostalim, po potrebi:

- Shemu klasifikacije podataka: kategorizacija osobnih podataka prema stupnju povjerljivosti na temelju zakonskih obveza ili samoprocjene;
- Zabranu neovlaštenog čitanja, preslikavanja, izmjena ili uklanjanja tijekom elektroničkog prijenosa ili prijevoza: osobito šifriranjem i preko virtualnih privatnih mreža (VPN);
- Sposobnost osiguranja stalne povjerljivosti, integriteta, dostupnosti i otpornosti sustava i usluga obrade;

110.0788.12 EU_HR/04.2022

- Zaštitu od slučajnog ili namjernog uništavanja ili gubitka, kao što su: strategija sigurnosnog rezervnog pohranjivanja (mrežno/izvan mreže; na lokalitetu/izvan lokaliteta), neprekidno napajanje električnom energijom (UPS, dizelski generator), antivirusni programi, vatrozid, kanali za uzbunu i planovi za hitne slučajeve; sigurnosne provjere na razini infrastrukture i aplikacija, sigurnosni plan na više razina s izmještenom uslugom sigurnosnih rezervnih pohranjivanja u rezervne podatkovne centre, standardni procesi u slučaju promjene/otpuštanja zaposlenika;
- mogućnost pravodobnog vraćanja dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta;
- postupak za redovito testiranje, procjenu i ocjenu učinkovitosti tehničkih i organizacijskih mjera za jamčenje sigurnosti obrade (interna revizija, PCI-DSS, ISO27001, nacionalne nadzorne ustanove);
- Obradu registara prema zahtjevima Opće uredbe o zaštiti osobnih podataka;
- Pristup uporabi sustava registriranja pristupa s relevantnim sposobnostima otkrivanja pokušaja neovlaštenog pristupa;
- Za glavnog kupca će Podaci i metapodaci (uključujući rezervno pohranjivanje, arhive, zapisnike u registru itd.) biti pohranjeni samo dok služe svrhama u koje su podaci prikupljeni, osim u slučaju zakonske ili ugovorne obveze zadržavanja podataka za dulje vremensko razdoblje.

H Kontrola organizacije

Obrađivač podataka održavat će svoju unutarnju organizaciju na način koji udovoljava uvjetima važećeg zakonodavstva i uvjetima za kontrolora podataka o sigurnosti podataka. To će se postići na sljedeći način:

Politikama i postupcima za internu obradu podataka, smjernicama, radnim uputama, opisima procesa i propisima za programiranje, ispitivanjima i objavljivanjima, ukoliko se odnose na Osobne podatke koje prenosi Kontrolor;

Provedbom okvira za kontrolu zaštite podataka koji podliježe godišnjoj reviziji usklađenosti;

Postojanje plan za hitne slučajeve s unaprijed određenim postupcima i raspodjelom odgovornosti (rezervni plan za nepredviđene slučajeve).