Tehnični in organizacijski ukrepi Worldline Financial Services (Europe) S.A.

(EU SL)

1 Namen tega dokumenta

Ta dokument vsebuje seznam tehničnih in operativnih ukrepov, ki veljajo kot standard. Dejanski sprejeti ukrepi so odvisni od storitve in kraja zadevne obdelave, saj niso vsi ukrepi ustrezni za vse storitve in lokacije. Worldline jamči, da ima za vse storitve in lokacije sprejete ustrezne tehnične in operativne ukrepe, navedene na spodnjem seznamu po oceni učinka o varstvu podatkov. Ukrepi so zasnovani za:

- zagotavljanje varnosti in zaupnosti osebnih podatkov,
- zaščito pred morebitnimi predvidenimi nevarnostmi ali grožnjam za varstvo in integriteto osebnih podatkov,
- zaščito pred vsemi dejanskimi nepooblaščenimi obdelavami, izgubami, uporabami, razkritji ali pridobitvami ali dostopi do osebnih podatkov.

Stran prav tako vsebuje seznam podizvajalcev, ki jih Worldline uporablja za izvajanje svojih storitev. Worldline jamči, da imajo vsi njeni podobdelovalci ustrezna zagotovila glede varstva osebnih podatkov, katere obdelujejo v našem imenu z izvajanjem kontrole podizvajalcev: izvajati se ne sme nobena obdelava podatkov v smislu 28. člena GDPR brez ustreznih navodil s strani glavnega subjekta, npr. jasne zasnove pogodbe, formaliziranega upravljanja podizvajalca in strogega izbora obdelovalcev (ISO certifikacija, ISMS) pred dokazovanjem usposobljenosti, spremljanje po izvedbi.
Banka Worldline je zavezana k nenehnemu spremljanju učinkovitosti svojih varovalk za informacije, prav tako pa je zavezana k vsakoletni reviziji s strani tretje osebe, ki predloži zagotovilo o veljavnih ukrepih in kontrolah.

2 Tehnični in organizacijski ukrepi

A Ljudje, ozaveščenost in človeški viri:

- Vsa zaposlovanja so podvržena postopku preverjanja glede na načela politike preverjanja preteklosti v banki Worldline;
- V vsaki pogodbi vsakega zaposlenega je klavzula sporazuma o nerazkritju informacij;
- Usposabljanje (in preizkus) na temo Etičnega kodeksa je vsakoletna obveznost vseh zaposlenih in se izvaja preko namenskega e-učnega modula;
- Vsi zaposleni prejmejo politiko za sprejemljivo uporabo IT v Skupini ali lokalno različico;
- Izjava o varnostni politiki, podpisana s strani upravnega odbora, je posredovana vsem zaposlenim;
- Osebje pri banki Worldline je dolžno upoštevati politiko varstva podatkov skupine Worldline na letni osnovi, prav tako pa mora opraviti usposabljanje (s preizkusom) na področju informacijske varnosti in varovanja;
- Redna usposabljanja na temo ozaveščanja o GDPR za vse zaposlene (poleg politike varstva podatkov skupine Worldline, usposabljanje na področju informacijske varnosti in varovanja);
- Dostop do sistemov se omogoči po načelu „po potrebi“, kjer se upošteva ločevanje nalog;
- Redne revizije notranjega varovanja se izvajajo za verifikacijo praks varnosti.

B Fizično varovanje in papirnate evidence:

Skladnost s politiko fizičnega in okoljskega varovanja skupine Worldline:

- Sistemi za nadzor dostopa in upravljanja z obiskovalci, ki so vzpostavljeni za vse obiskovalce/goste;
- Nadzor fizičnega dostopa (varovanje pred nepooblaščenim dostopom do prostorov za obdelavo podatkov ali hrambe podatkov): še posebej v obliki magnetnih ali pametnih kartic, električnih odpiralcev vrat, vratarjev, varnostnega osebja, alarmnih sistemov, video sistemov.
- Pregledi fizičnih dostopov glede na opredeljeno periodičnost;
- Uveden postopek čiste mize, praznega zaslona in tiskanja s fizično prisotnostjo;
- Informacije, ki vključujejo papirne dokumente, s katerimi rokuje uvoznik podatkov, so zaupne, označene, zaščitene in z njimi se upravlja v skladu s politiko o klasifikaciji informacij skupine Worldline;
- Namiznih računalnikov se ne odstranjuje z lokacije, razen če je za to bila podana posebna predhodna avtorizacija;
- Video nadzor za varovanje omejenih območij;
- Uvedeni požarni sistemi za varnost zaposlenih;
- Evakuacijske vaje se izvajajo tako pogosto, kot je opredeljeno;

C Naprave za dostop na daljavo so zaščitene:

Uporabniki, ki delo opravljajo na daljavo, le-tega opravljajo na prenosnih in namiznih računalnikih preko varnega omrežja skupine Worldline, s katerim upravlja Global IT za skupino Worldline. Poleg tega so uvedeni naslednji varnostni ukrepi:

- Šifriranje trdega diska na službenih prenosnih računalnikih;
- Dvofaktorska avtentikacija (PKI/alternativa);
- Centralno upravljana in protivirusna zaščita;
- Upravljanje in spremljanje programske opreme za nadzor namestitve avtorizirane programske opreme;
- Uvedeno načelo vnosa ID in gesla za dostop do informacij;
- Uvedeni so periodični pregledi dostopa;
- E-pošta se samodejno preverja s protivirusno programsko opremo in programsko opremo za varovanje pred neželeno pošto.

D Varnost dostopa na daljavo

Dvofaktorska identifikacija se uporabi na splošno pri dostopu na daljavo do kritičnih tarčnih sistemov skupine Worldline. Če je vir povezave na daljavo sistem, katerega nadzira banka Worldline, potem avtentikacija naprave temelji na certifikatu na napravi.
Vse morebitne druge povezave mora najprej odobriti oddelek za varnost.

E Splošni varnostni ukrepi:

- Podatki se shranjujejo v podatkovnih centrih EU in Švice oz. na lokalnih napravah (prenosnikih);
- Prekinitev dostopa na demilitariziranem območju;
- Vse povezave do varovanega (PCI) območja so šifrirane;
- Dostop do PCI območja je možen samo preko močne avtentikacije preko ponujenega varnostnega odjemalca;
- Potrebno je iti skozi številne sloje požarnih zidov in detektorjev motenj;
- Dostop se upravlja glede na načela dostopa, ki temeljijo na vlogah.
- Varovanje zasebnosti, vključno z rednim usposabljanjem zaposlenih;
- Upravljanje z varnostnimi incidenti;
- Privzete nastavitve, ki upoštevajo zasebnost

F Nadzor dostopa do osebnih podatkov

Zaposleni, ki imajo dostop do zasebnih podatkov, lahko dostopajo le do tistih podatkov, ki so potrebni za namen in dejavnosti, za katere so odgovorni. Avtorizacija dostopa se omogoči po načelu „po potrebi“ in „potrebe dostopa“ in temelji bodisi na vlogi, bodisi na imenu. Vodijo se dnevniki dostopa, prav tako pa je dodeljena odgovornost za nadzor dostopa.

Vzpostavljeni so naslednji ukrepi:

- Dolžnost zaposlenih, da delujejo v skladu z veljavnimi politikami lokalne varnosti in politikami varstva podatkov, ki veljajo za skupino Worldline;
- Delovna navodila o rokovanju z zasebnimi podatki;
- Elektronski nadzor dostopa (zaščita pred nepooblaščeno uporabo sistemov za obdelavo ali hrambo podatkov): še posebej na podlagi gesel (in tudi ustrezne politike), mehanizmov samodejnega zaklepa, dvofaktorske avtentikacije, šifriranja podatkovnih nosilcev;
- Interni nadzor dostopa (preprečevanje nepooblaščenega branja, kopiranja, spreminjanja ali odstranjevanja podatkov v banki Worldline): z uporabo standardnih avtorizacijskih profilov na „po potrebi“, standardnih postopkov za dodeljevanje uporabniških pravic, beleženja prijav, periodičnega pregleda dodeljenih pravic, še posebej administratorskih računov;
- Nadzorovano uničenje podatkovnih medijev;
- Uvedeni so postopki za preverjanje skladnosti s postopki in delovnimi navodili;

G Varnost in zaupnost osebnih podatkov

Banka Worldline bo na podlagi ocene tveganja (in po potrebi dodatnega DPIA) zagotovila stopnjo varnosti, ki bo primerna za tveganje, med drugim tudi:

- Klasifikacijsko shemo za podatke: kategorizacija osebnih podatkov glede na stopnjo zaupnosti na podlagi pravnih obveznosti ali samoocene.
- Nič nepooblaščenega branja, kopiranja, spreminjanja ali odstranjevanja pri elektronskem prenosu ali transportu: še posebej na podlagi šifriranja in VPN (virtualna zasebna omrežja oz. Virtual Private Network);
- sposobnost zagotavljanja stalne zaupnosti, integritete, razpoložljivosti in odpornosti sistemov in storitev obdelave podatkov;

110.0788.10 EU_SL/04.2022

- Varovanje pred nenamernim ali namernim uničenjem ali izgubo, kot npr. strategija varnostnega kopiranja (spletnega/brez povezave; na lokaciji/izven lokacije), brezprekinitveno napajanje (UPS, komplet dizelskih generatorjev), protivirusna zaščita, požarni zid, opozorilni kanali in načrti za ukrepanje v sili; varnostna preverjanja infrastrukture in aplikacijskih ravni, večstopenjski varnostni načrt z varnostnim kopiranjem podatkov v za to namenjene centre, standardni postopki v primeru zamenjave/odpustitve zaposlenih;
- sposobnost pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta;
- postopek za redno testiranje, ocenjevanje in vrednotenje učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave (notranja revizija, PCI-DSS, ISO27001, nacionalne nadzorne institucije).
- Registri postopkov glede na zahteve GDPR
- Uporaba dnevnikov dostopov do sistemov z namenom zaznavanja poskusov nepooblaščenega dostopa
- Podatki in metapodatki glavnih strank (tudi varnostno kopiranje, arhiviranje, dnevniki, itd) bodo hranjeni samo tako dolgo, dokler izpolnjujejo namen, za katerega so bili zbrani, razen če obstaja pravna ali pogodbena dolžnost za hrambo teh podatkov za dlje časa.

H Organizacijski nadzor

Obdelovalec podatkov bo ohranjal svojo interno organizacijo na način, ki je skladen z zahtevami veljavne zakonodaje in zahtevami upravljavcev podatkov na področju varstva podatkov. To se zagotovi s/z:

Internimi politikami obdelave podatkov in postopki, smernicami, delovnimi navodili, opisi postopkov in predpisi za programiranje, testiranje in izdajanje v primerih, ko se le-ti nanašajo na osebne podatke, ki jih prenese upravljavec podatkov;

Izvajanjem okvirja nadzora varstva podatkov, katerega skladnost se revidira vsako leto;

Z vzpostavitvijo zasilnega načrta s postopki in porazdelitvijo odgovornosti (rezervni krizni načrt).