Technische en organisatorische maatregelen Worldline Financial Services (Europe) S.A.

(EU NL)

1 Doel van dit document

Dit document bevat een lijst van de technische en operationele maatregelen die standaard van toepassing zijn. De maatregelen die daadwerkelijk worden getroffen, zijn afhankelijk van de Dienst en de locatie van verwerking, aangezien niet alle maatregelen relevant zijn voor alle Diensten en locaties. Worldline garandeert dat voor alle Diensten en locaties de noodzakelijke adequate technische en veiligheidsmaatregelen zijn getroffen; deze zijn opgenomen in onderstaande lijst naar aanleiding van een Data Protection Impact Assessment. De maatregelen zijn bedoeld om:

- de veiligheid en vertrouwelijkheid van Persoonsgegevens te waarborgen,
- te beschermen tegen alle verwachte bedreigingen of gevaren voor de veiligheid en integriteit van Persoonsgegevens,
- te beschermen tegen het ongeoorloofd verwerken, onthullen, verkrijgen of raadplegen van Persoonsgegevens en tegen verlies en niet-toegestaan gebruik van Persoonsgegevens.

De pagina bevat ook een lijst van onderaannemers waarop Worldline een beroep doet voor het verlenen van haar diensten. Worldline garandeert dat al haar subverwerkers voldoende garanties hebben geboden voor de bescherming van persoonsgegevens die zij namens ons verwerken door controle op de onderaanneming uit te oefenen: er mag geen gegevensverwerking in opdracht plaatsvinden in de zin van AVG art. 28 zonder passende instructies van de opdrachtgever, d.w.z. een duidelijk contractontwerp, geformaliseerd beheer van de onderaanneming en een strenge selectie van verwerkers (ISO-certificering, managementsysteem voor informatiebeveiliging), het vooraf aantonen van competenties en follow-upbewaking.
Worldline verbindt zich ertoe om continu toezicht te houden op de effectiviteit van haar informatiebeveiliging en een jaarlijkse conformiteitscontrole te laten uitvoeren door een derde om zekerheid te verschaffen over de getroffen maatregelen en controles.

2 Technische en organisatorische maatregelen

A Mensen, bewustwording en HR:

- Bij elke werving wordt een screeningproces gevolgd overeenkomstig de principes van het beleid dat Worldline hanteert voor antecedentenonderzoek,
- In elke overeenkomst met elke werknemer zijn geheimhoudingsbepalingen opgenomen,
- Een bewustwordingstraining over de Ethische Code (inclusief een test) is een jaarlijkse verplichting voor alle werknemers en wordt aangeboden in de vorm van een e-learningmodule over dit onderwerp,
- Het groepsbeleid Acceptabel Gebruik van IT of een lokale versie wordt gedeeld met alle werknemers,
- Een door het management ondertekende verklaring over veiligheidsbeleid wordt gedeeld met alle werknemers,
- Het personeel van Worldline is verplicht om jaarlijks de training over het Gegevensbeschermingsbeleid van Worldline, Informatiebeveiliging en Veiligheid te volgen (inclusief een test),
- Regelmatige bewustwordingstrainingen over de AVG voor alle werknemers (in aanvulling op de training over het Gegevensbeschermingsbeleid van Worldline, Informatiebeveiliging en Veiligheid),
- Toegang tot systemen wordt verleend op basis van 'need to know', met inachtneming van de scheiding van taken,
- Er worden regelmatig interne veiligheidsaudits uitgevoerd om de veiligheidspraktijken te verifiëren.

B Fysieke beveiliging en papieren dossiers:

Naleving van het Worldline-beleid voor Fysieke en Milieubeveiliging:

- Toegangscontrole en systemen voor bezoekersbeheer geïmplementeerd voor alle bezoekers/gasten,
- Fysieke toegangscontrole (bescherming tegen ongeoorloofde toegang tot gegevensverwerkings- of opslagfaciliteiten): met name via magnetische kaarten of smartcards, elektrische deuropeners, een portier, veiligheidspersoneel, alarmsystemen, videosystemen.
- Revisies van fysieke toegang met de vastgestelde frequentie,
- Procedure voor 'schoon bureau, schoon scherm en follow-me-printing' geïmplementeerd,
- Informatie die door de gegevensimporteur wordt verwerkt, waaronder papieren documenten, wordt geclassificeerd, gelabeld, beschermd en verwerkt in overeenstemming met het Worldline-beleid voor informatieclassificatie;
- Desktopcomputers mogen de locatie niet verlaten, behalve met specifieke voorafgaande toestemming,
- CCTV-toezicht om verboden zones te beveiligen,
- Brandalarm- en brandbestrijdingssystemen geïmplementeerd voor de veiligheid van werknemers,
- Er worden met vaste tussenpozen brandevacuatieoefeningen gehouden.

C Apparaten van eindgebruikers op afstand worden beschermd:

Gebruikers die op afstand werken, werken met een laptop en desktopcomputer op het beveiligde netwerk van Worldline, dat door de wereldwijde IT-afdeling wordt onderhouden voor de Worldline Groep. Daarnaast worden de volgende veiligheidsmaatregelen toegepast:

- Versleuteling van de harde schijf op door het bedrijf toegewezen laptops,
- Tweefactorauthenticatie (PKI/alternatief),
- Centraal beheerde en antivirusbescherming,
- Beheer en bewaking van de software om ongeoorloofde installatie van software te voorkomen,
- Controles van inlognaam en wachtwoord geïmplementeerd voor de toegang tot informatie,
- Periodieke toegangsrevisie geïmplementeerd,
- E-mails worden automatisch gescand op antivirus- en antispamsoftware.

D Beveiliging bij toegang op afstand

In het algemeen wordt tweefactorauthenticatie gebruikt voor toegang op afstand tot kritieke Worldline-doelsystemen. Als de verbinding op afstand tot stand wordt gebracht met een door Worldline gecontroleerd systeem, wordt authenticatie op basis van een certificaat op het apparaat geïmplementeerd.
Elke andere configuratie van verbindingen moet vooraf worden goedgekeurd door de veiligheidsafdeling.

E Algemene veiligheidsmaatregelen zijn o.a.:

- Gegevens worden bewaard in datacentra in de EU en Zwitserland, of in het geval van laptops, versleuteld op het lokale apparaat,
- Beëindiging van toegangsverbinding in gedemilitariseerde zones,
- Alle verbindingen tot aan het beveiligde gebied (PCI-zone) zijn versleuteld,
- Toegang tot PCI-zones is alleen mogelijk via sterke authenticatie middels een verstrekte beveiligingsclient,
- Meerdere lagen van firewalls en indringingsdetectie moeten worden gepasseerd,
- Toegang beheerd volgens de principes van rolgebaseerde toegangscontrole,
- Privacymanagement, inclusief regelmatige trainingen van werknemers,
- Incidentresponsbeheer,
- Privacyvriendelijke standaardinstellingen.

F Toegangscontrole voor Persoonsgegevens

Werknemers met toegang tot privégegevens hebben alleen toegang tot de gegevens die noodzakelijk zijn voor de taken onder hun verantwoordelijkheid. Toegang wordt verleend op basis van de 'need to know'- en 'need to access'-beginselen en is ofwel rolgebaseerd, ofwel naamgebaseerd. Er zijn toegangslogboeken aanwezig en er worden werknemers verantwoordelijk gesteld voor toegangscontrole.

De volgende maatregelen zijn ingevoerd:

- Verplichting voor werknemers om zich te houden aan het toepasselijke lokale veiligheids- en gegevensbeschermingsbeleid en het veiligheids- en gegevensbeschermingsbeleid van Worldline,
- Werkinstructies over de verwerking van privégegevens,
- Elektronische toegangscontrole (bescherming tegen ongeoorloofd gebruik van gegevensverwerkings- of opslagsystemen): met name via wachtwoorden (inclusief het bijbehorende beleid), automatische vergrendelingsmechanismen, tweefactorauthenticatie, versleuteling van gegevensdragers,

110.0788.07 EU_NL/04.2022

- Interne toegangscontrole (preventie van het ongeoorloofd lezen, kopiëren, wijzigen of verwijderen van gegevens binnen Worldline): door het gebruik van standaardautorisatieprofielen op basis van 'need to know', een standaardproces voor toewijzing van gebruikersrechten, logboekregistratie van toegangsactiviteiten, periodieke herziening van de toegewezen rechten, met name van beheerdersaccounts,
- Gecontroleerde vernietiging van gegevensdragers,
- Er zijn procedures voor controle van de naleving van procedures en werkinstructies aanwezig.

G Veiligheid en vertrouwelijkheid van persoonsgegevens

Op basis van een risicobeoordeling (en indien nodig een aanvullende DPIA) zorgt Worldline voor een beveiligingsniveau dat past bij het risico, waaronder voor zover van toepassing:

- Classificatieschema voor gegevens: categorisering van persoonsgegevens overeenkomstig de mate van vertrouwelijkheid, op basis van wettelijke verplichtingen of zelfstandige beoordeling,
- Lezen, kopiëren, wijzigen of verwijderen is niet toegestaan tijdens elektronische verzending of transport; dit wordt met name gewaarborgd via versleuteling en Virtual Private Networks (VPN),
- het vermogen om de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en diensten te waarborgen,
- Bescherming tegen vernietiging of verlies, onbedoeld of opzettelijk, waaronder via een back-upstrategie (online/offline, op locatie/elders), Uninterruptible Power Supply (UPS, dieselgenerator), antivirus, firewall, waarschuwingskanalen en noodplannen, veiligheidscontroles op het niveau van de infrastructuur en toepassingen, meerlaags beveiligingsplan met uitbesteding van back-ups aan gegevensback-upcentra, standaardprocessen in geval van vervanging/ontslag van werknemers,
- het vermogen om de beschikbaarheid en toegang tot Persoonsgegevens tijdig te herstellen in geval van een fysiek of technisch incident,
- een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de veiligheid van de verwerking te waarborgen (interne audits, PCI-DSS, ISO27001, nationale toezichthoudende instanties),
- Verwerkingsregisters die voldoen aan de eisen van de AVG,
- Gebruik van toegangslogsystemen die relevant zijn om ongeoorloofde toegangspogingen te detecteren,
- De belangrijkste klantgegevens en metagegevens (waaronder back-ups, archieven, logbestanden, enz.) worden slechts bewaard zolang dat noodzakelijk is voor de doelen waarvoor de gegevens werden verzameld, tenzij er een wettelijke of contractuele verplichting bestaat om de gegevens langer te bewaren.

H Organisatorische controle

De Gegevensverwerker onderhoudt zijn interne organisatie op een manier die voldoet aan de voorschriften van de toepasselijke wetgeving en de eisen van de Verwerkingsverantwoordelijke ten aanzien van gegevensbescherming. Dit wordt gedaan via:

Intern beleid en interne procedures voor gegevensverwerking, richtlijnen, werkinstructies, procesbeschrijvingen en voorschriften voor programmeren, testen en vrijgeven, voor zover deze betrekking hebben op de Persoonsgegevens die de Verwerkingsverantwoordelijke overdraagt;

Implementeren van een controlekader voor Gegevensbescherming dat jaarlijks wordt gecontroleerd op conformiteit;

Aanwezigheid van een noodplan met procedures en toewijzing van verantwoordelijkheden (back-upnoodplan).