MERCHANT SERVICES TECHNISCHE EN ORGANISATORISCHE MAATREGELEN ("TOMS")

Dit document bevat een lijst van de standaard technische en organisatorische maatregelen die van toepassing zijn. Deze lijst kan worden aangevuld met aanvullende maatregelen die worden beschreven in de toepasselijke Dienst Voorwaarden. De maatregelen zijn ontworpen om:

- de veiligheid en vertrouwelijkheid van Persoonsgegevens te waarborgen;
- te beschermen tegen alle voorzienbare bedreigingen of gevaren voor de veiligheid en integriteit van Persoonsgegevens;
- te beschermen tegen elke daadwerkelijke ongeautoriseerde verwerking, verlies, gebruik, openbaarmaking of verkrijging van of toegang tot Persoonsgegevens.

Worldline verbindt zich ertoe de effectiviteit van haar beveiligingsmaatregelen continu te monitoren en haar PCI DSS level 1 compliance status te handhaven.

1. PERSONEN, BEWUSTZIJN EN HUMAN RESOURCES (HR):

1.1. Alle aanwervingen volgen een screeningsproces volgens de principes van het beleid inzake achtergrondcontrole van de Worldline Groep, binnen de grenzen van de lokale wetgeving.

1.2. In hun contract hebben alle werknemers vertrouwelijkheids- en geheimhoudingsverplichtingen.

1.3. Er is een verplichte jaarlijkse bewustwordingstraining over de Gedragscode (inclusief een toets) voor alle personeel.

1.4. Het personeel van Worldline is jaarlijks verplicht om de volgende trainingen te volgen (inclusief een toets): Gegevensbescherming, Informatiebeveiliging & Veiligheid, en PCI DSS Security training.

1.5. Het beveiligingsbeleid en het gegevensbeschermingsbeleid worden gedeeld met alle werknemers.

1.6. Werknemers zijn verplicht om te voldoen aan het toepasselijke beveiligings- en gegevensbeschermingsbeleid van de Worldline Groep en het lokale beleid.

1.7. Er is regelmatige bewustwordingscommunicatie over de Algemene Verordening Gegevensbescherming (AVG) voor alle personeel (naast het Gegevensbeschermingsbeleid en de Informatiebeveiligings- en Veiligheidstraining).

1.8. Er worden extra specifieke trainingen door de gegevensbescherming community aangeboden aan geselecteerde teams en werknemers.

2. ORGANISATIEREGELING:

Worldline zal haar interne organisatie zodanig inrichten dat deze voldoet aan de eisen van de toepasselijke wet- en regelgeving en aan de vereisten van de Gegevensverantwoordelijke op het gebied van gegevensbeveiliging. Dit zal worden gerealiseerd door:

2.1. het aanstellen van een Functionaris voor Gegevensbescherming ("DPO");

2.2. een organisatie en governance voor Gegevensbescherming, Beveiliging en Bedrijfscontinuïteit;

2.3. een uitgebreid netwerk van gegevensbeschermingsexperts van Atos en Worldline;

2.4. rollen en verantwoordelijkheden m.b.t. gegevensbescherming voor alle medewerkers;

2.5. beleidsnormen die de privacy en beveiliging van gegevens regelen;

2.6. een intern gegevensverwerkingsbeleid, procedures en processen voor codering, testen, wijzigingen en releases, voor zover deze betrekking hebben op de verwerkte Persoonsgegevens;

2.7. de implementatie van een gegevensbeschermingscontrolekader dat periodiek wordt beoordeeld op naleving;

2.8. regelmatige interne veiligheidsaudits om de beveiligingspraktijken te verifiëren;

2.9. waarborgen dat dezelfde technische en organisatorische maatregelen worden toegepast bij leveranciers die Persoonsgegevens verwerken;

2.10. de PCI DSS norm (*Payment Card Industry Data Security Standard*) voor de bescherming van kaartgegevens.

3. FYSIEKE BEVEILIGING EN VEILIGHEID, DOCUMENTENBEHEER:

Alle entiteiten binnen de Worldline Groep voldoen aan de "Group Worldline Physical and Environmental Security Policy & Information Protection Standard":

3.1. fysieke toegangscontrole is geïmplementeerd voor alle medewerkers, en er zijn beheersystemen voor bezoekers en gasten;

3.2. er worden regelmatig controles op fysieke toegang uitgevoerd volgens een bepaalde frequentie;

3.3. informatie, inclusief papieren documenten, wordt geclassificeerd, gelabeld, beschermd en afgehandeld volgens het informatieclassificatiebeleid van Worldline;

3.4. specifieke regels bepalen hoe informatie te bewaren, verwerken, tonen, afdrukken, overdragen en vernietigen (zowel in elektronische als papieren vorm);

3.5. CCTV-beveiliging wordt gebruikt om beveiligde gebieden te bewaken;

3.6. brandbeveiligingssystemen, wateroverlastbeveiliging, verwarmings-, airconditioning- en stroomback-upsystemen zijn aanwezig om de integriteit en beschikbaarheid van gegevens in de datacentra te waarborgen;

3.7. gecontroleerde vernietiging van gegevensmedia wordt zorgvuldig uitgevoerd.

4. TECHNISCHE INFRASTRUCTUUR EN BEVEILIGING VAN APPLICATIES:

Worldline heeft een security-architectuur met meervoudige verdedigingslagen geïmplementeerd, wat zorgt voor een gelaagde beveiliging. De volgende beveiligingsmaatregelen zijn van toepassing:

4.1. netwerkscheiding en -segmentatie;

4.2. beveiligde verzending van gegevens over niet-vertrouwde netwerken;

4.3. Persoonsgegevens worden opgeslagen op productie-netwerken die worden gescheiden door middel van firewalls;

4.4. IDS (Inbraakdetectiesysteem) en IPS (Inbraakpreventiesysteem) – evenals monitoring via SIEM (Security Information and Event Management);

4.5. beveiligingsgateways en VPN-oplossingen voor externe verbindingen;

4.6. vulnerability management, patchmanagement en veilige configuraties;

4.7. penetratietests voor applicaties;

4.8. Web Application Firewall (WAF);

4.9. secure coding praktijken;

4.10. gegevens worden uitsluitend opgeslagen in EU-datacentra en, in het geval van laptops, versleuteld op het lokale apparaat.

5. **BESCHERMING VAN END-USER APPARATEN:**

Werknemers van Worldline werken met laptops/desktops op het beveiligde netwerk van Worldline. De volgende beveiligingsmaatregelen zijn geïmplementeerd:

5.1. versleuteling van de harde schijf op toegewezen laptops;

5.2. twee-factor authenticatie (PKI of alternatief) voor remote werken;

5.3. centraal beheerde antivirusbescherming, patchmanagement, firewall en host intrusion prevention systeem;

5.4. beheer en monitoring van software om ongeautoriseerde software-installaties te voorkomen;

5.5. beveiligd beheer van de levenscyclus van apparaten.

6. **BEVEILIGING VAN REMOTE TOEGANG:**

Twee-factor authenticatie wordt gebruikt voor remote toegang tot de kritieke systemen van Worldline. Voor systemen die door Worldline worden beheerd, wordt een VPN oplossing (Virtual Private Network) ingezet om verbinding te maken met het Worldline-netwerk. Voor niet-beheerde systemen is daarnaast een VDI oplossing (Virtual Desktop Infrastructure) geïmplementeerd. Elke andere setup van verbindingen moet vooraf worden goedgekeurd door de beveiligingsafdeling.

7. **BESCHERMING VAN DE TOEGANG TOT PERSOONSGEGEVENS:**

Medewerkers met toegang tot Persoonsgegevens kunnen alleen toegang krijgen tot de gegevens die noodzakelijk zijn voor de uitvoering van de activiteiten onder hun verantwoordelijkheid. Toegangsautorisatie wordt verleend op basis van het principe van 'least privilege' en is ofwel gebaseerd op de rol of op naam vastgesteld. Toegangslogboeken en audit-trails zijn aanwezig, en de verantwoordelijkheid voor toegangscontrole is toegewezen.

8. **BEVEILIGING, GEHEIMHOUDING, BESCHIKBAARHEID VAN PERSOONSGEGEVENS:**

Op basis van een risicoanalyse (en indien nodig een aanvullende gegevensbeschermingseffectbeoordeling (“Data Protection Impact Assessment” of “DPIA”) zal Worldline zorgen voor een beveiligingsniveau dat geschikt is voor het risico, inclusief o.a., indien passend:

8.1. het anonimiseren en versleutelen van Persoonsgegevens;

8.2. het waarborgen van de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssyste(e)m(en) en diensten;

8.3. het vermogen om de beschikbaarheid en toegang tot Persoonsgegevens tijdig te herstellen in geval van een fysieke of technische verstoring;

8.4. een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de verwerking te verzekeren;

8.5. een logische scheiding van klantgegevens verzekeren;

8.6. het opzetten van een proces om verwerkte gegevens accuraat en up-to-date te houden;

8.7. het bijhouden van verwerkingsactiviteiten volgens de AVG;

8.8. het implementeren van maatregelen ter detectie van onbevoegde toegang via toegangslogboeken;

8.9. klantgegevens (inclusief back-ups en archieven) worden alleen bewaard zolang dit nodig is voor de doeleinden waarvoor de gegevens verzameld zijn, conform de instructies van de klant, tenzij er een wettelijke of contractuele verplichting is om de gegevens langer te bewaren;

8.10. incidentmanagementproces en incidentresponseplannen;

8.11. een procedure voor het melden van datalekken;

8.12. plannen voor calamiteiten en rampenherstel met procedures en toewijzing van verantwoordelijkheden (backup-contingency plan).