Mesures techniques et organisationnelles Worldline Financial Services (Europe) S.A.

(EU FR)

1 Objet du présent Document

Le présent Document contient une liste des mesures techniques et opérationnelles applicables en tant que norme. Les mesures effectivement prises dépendent du Service et du site de traitement concerné, car toutes les mesures ne sont pas pertinentes pour tous les Services et sites. Worldline garantit qu'elle dispose, pour tous les Services et sites, des mesures techniques et opérationnelles adéquates nécessaires énoncées dans la liste ci-dessous à la suite d'une Évaluation d'incidence sur la Protection des données. Les mesures sont conçues pour :

- assurer la sécurité et la confidentialité des Données personnelles ;
- protéger contre tout(e) menace ou danger anticipé(e) par rapport à la sécurité et à l'intégrité des Données personnelles ;
- protéger contre tout(e) traitement, perte, utilisation, divulgation, acquisition ou accès non autorisé à toute Donnée Personnelle

La page contient également une liste de sous-traitants auxquels recourt Worldline pour la prestation de ses services. Worldline s'assure que tous ses sous-traitants ont fourni des garanties adéquates relativement à la Protection des données personnelles qu'ils traitent en son nom en effectuant un contrôle des sous-traitants : il ne peut y avoir de traitement de données commandé au sens de l'art. 28 RGPD sans instructions appropriées du donneur d'ordre, par exemple, conception claire du contrat, gestion formalisée de la sous-traitance et sélection rigoureuse des sous-traitants (certification ISO, SGSI), démonstration préalable de compétence, contrôle de suivi.
Worldline s'engage à contrôler en permanence l'efficacité de ses mesures de protection des informations et à faire effectuer un audit de conformité annuel par un tiers pour apporter une assurance quant aux mesures et contrôles en place.

2 Mesures techniques et organisationnelles

A Personnel, sensibilisation et RH :

- Tous les recrutements suivent un processus de sélection selon les principes de la politique de Worldline en matière de vérification des antécédents ;
- Tout contrat conclu avec tout travailleur comporte des clauses de confidentialité ;
- Une formation de sensibilisation au Code d'éthique (test compris) est une obligation annuelle pour tous les travailleurs et doit être suivie sur la base d'un module e-learning dédié ;
- La Politique d'utilisation acceptable de l'informatique du Groupe ou sa version locale est partagée avec tous les travailleurs ;
- La Déclaration de politique de sécurité signée par la Direction est partagée avec tous les travailleurs ;
- Le personnel de Worldline est tenu de suivre chaque année la Politique de Protection des données de Worldline et la formation à la sécurité et à la sûreté des informations (test compris) ;
- Des formations régulières de sensibilisation au RGPD pour tous les travailleurs (en plus de la Politique de Protection des données de Worldline et de la formation à la sécurité et à la sûreté des informations) ;
- L'accès aux systèmes est donné sur la base d'un « besoin d'accès », en tenant compte de la séparation des tâches ;
- Des audits de sécurité internes réguliers sont menés pour vérifier les pratiques en matière de sécurité.

B Sécurité physique et registres papier :

Conformité avec la Politique de sécurité physique et environnementale du Groupe Worldline :

- Systèmes de contrôle d'accès et de gestion des visiteurs mis en œuvre pour tous les visiteurs/invités ;
- Contrôle d'accès physique (protection contre l'accès non autorisé aux installations de traitement ou de stockage des données) : en particulier au moyen de cartes magnétiques ou à puce, d'ouvre-portes électriques, de portiers, de personnel de sécurité, de systèmes d'alarme et de systèmes vidéo.
- Examens d'accès physique selon la périodicité définie ;
- Bureau net, écran net et impression sécurisée, processus mis en œuvre ;
- Les informations, y compris les documents papier, traitées par l'importateur de données sont classées, étiquetées, protégées et traitées conformément à la Politique de classification des informations de Worldline ;
- Sauf autorisation spécifique préalable, les ordinateurs de bureau ne sortent pas du site ;
- Surveillance CCTV pour protéger les zones à accès restreint ;
- Systèmes d'alarme incendie et de lutte contre l'incendie mis en œuvre pour la sécurité des travailleurs ;
- Des exercices d'évacuation en cas d'incendie sont menés à des fréquences spécifiées ;

C Les appareils des utilisateurs finaux distants sont protégés :

Les utilisateurs distants travaillent avec un ordinateur portable et un ordinateur de bureau sur le réseau sécurisé Worldline maintenu par Global IT pour le Groupe Worldline. Les mesures de sécurité suivantes sont intégrées en plus :

- Cryptage du disque dur sur les ordinateurs portables affectés à l'entreprise ;
- Authentification à 2 facteurs (ICP/AIternative) ;
- Protection antivirus à gestion centralisée ;
- Gestion et surveillance du logiciel pour contrôler une installation logicielle autorisée ;
- Des contrôles d'identifiant de connexion et de mot de passe sont mis en œuvre pour l'accès aux informations ;
- Un examen périodique des accès est mis en œuvre ;
- Les e-mails sont automatiquement analysés par un logiciel anti-virus et anti-spam.

D Sécurité des accès distants

L'authentification à 2 facteurs est généralement utilisée pour l'accès distant aux systèmes cibles critiques de Worldline. Si la source de la connexion distante est un système contrôlé par Worldline, l'authentification de l'appareil fondée sur un certificat sur l'appareil est mise en œuvre.
Toute autre configuration de connexions doit être préalablement approuvée par le service sécurité.

E Les mesures de sécurité génériques sont notamment :

- Les données sont stockées dans les centres de données de l'UE et de Suisse ou, dans le cas des ordinateurs portables, cryptés sur l'appareil local ;
- Fin de la connexion d'accès en zone démilitarisée ;
- Toute la connectivité jusqu'à la zone sécurisée (zone PCI) est cryptée ;
- L'accès à la zone PCI n'est possible qu'avec une authentification forte via le client de sécurité fourni ;
- Plusieurs couches de pare-feu et de détection d'intrusion doivent être franchies ;
- Accès géré selon les principes du contrôle d'accès fondé sur les rôles ;
- Gestion de la confidentialité, y compris la formation régulière des travailleurs ;
- Gestion des réponses aux incidents ;
- Paramètres par défaut respectueux de la confidentialité ;

F Contrôle d'accès aux Données personnelles

Les travailleurs ayant accès aux données privées ne peuvent accéder qu'aux données nécessaires aux activités qui relèvent de leur responsabilité. L'autorisation d'accès est donnée en fonction du « besoin de savoir » et du « besoin d'accès » et repose sur le rôle ou sur le nom. Des journaux d'accès sont en place et la responsabilité du contrôle d'accès est attribuée.

Les mesures suivantes sont en place :

- Obligation pour les travailleurs de se conformer aux politiques de sécurité et aux politiques de Protection des données applicables de Worldline ou locales ;
- Des instructions de travail pour le traitement des données privées ;
- Un contrôle d'accès électronique (protection contre l'utilisation non autorisée des systèmes de traitement ou de stockage des données) : en particulier, par mots de passe (y compris la politique correspondante), des mécanismes de verrouillage automatique, une authentification à deux facteurs, le cryptage des supports de données ;
- Contrôle d'accès interne (prévention de la lecture, de la copie, de la modification ou de la suppression de données non autorisées au sein de Worldline) : à savoir, en utilisant des profils d'autorisation standard sur la base du « besoin de savoir », un processus standard pour l'attribution des droits d'utilisateur, la journalisation des accès, la révision périodique des droits cédés, en particulier des comptes administrateurs ;

110.0788.03 EU_FR/04.2022

- Destruction contrôlée des supports de données ;
- Des procédures de vérification du respect des procédures et des instructions de travail sont en place ;

G Sécurité et confidentialité des Données personnelles

Sur la base d'une évaluation des risques (et si nécessaire d'une EIPD supplémentaire), Worldline garantira un niveau de sécurité approprié au risque, y compris, entre autres, le cas échéant :

- Schéma de classification des données : catégorisation des Données personnelles selon le degré de confidentialité sur la base d'obligations légales ou d'une auto-évaluation ;
- Absence de lecture, de copie, de modification ou de suppression non autorisée lors de la transmission ou du transport électronique : en particulier, par cryptage et réseaux privés virtuels (VPN) ;
- La capacité d'assurer en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;
- Protection contre la destruction ou la perte accidentelle ou intentionnelle, telle que stratégie de sauvegarde (en ligne/hors ligne ; sur site/hors site), alimentation sans interruption (UPS, groupe électrogène au diesel), antivirus, pare-feu, canaux d'alerte et plans d'urgence ; contrôles de sécurité au niveau de l'infrastructure et des applications, plan de sécurité multi-niveaux avec externalisation des sauvegardes vers des centres de sauvegarde des données, processus standard en cas de changement/licenciement de travailleurs ;
- La possibilité de restaurer la disponibilité et l'accès aux Données personnelles en temps opportun en cas d'incident physique ou technique ;
- Un processus pour tester et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles en vue d'assurer la sécurité du traitement (audit interne, PCI-DSS, ISO27001, institutions nationales de surveillance) ;
- Traiter les registres conformément aux exigences du RGPD ;
- L'utilisation de systèmes de journaux d'accès est pertinente aux fins de détecter les tentatives d'accès non autorisé ;
- Pour le client principal, les données et métadonnées (y compris les sauvegardes, les archives, les fichiers journaux, etc.) ne seront conservées qu'aussi longtemps qu'elles serviront les objectifs pour lesquels les données ont été collectées, sauf s'il existe une obligation légale ou contractuelle de conserver les données pendant une période plus longue.

H Contrôle de l'organisation

Le Sous-traitant de données doit maintenir son organisation interne d'une manière qui répond aux exigences de la législation applicable et aux exigences du Responsable du traitement des données en matière de sécurité des données. Ceci doit être accompli au moyen de :

Politiques et procédures internes de traitement des données, directives, instructions de travail, descriptions des processus et réglementations pour la programmation, tests et diffusion, dans la mesure où ils concernent les Données personnelles transférées par le Responsable ;

La mise en œuvre d'un cadre de contrôle de la Protection des données dont la conformité est auditée annuellement ;

Un plan d'urgence comportant des procédures et une répartition des responsabilités (plan d'urgence de secours).