Nos engagements en tant que sous-traitant

Résumé des mesures techniques et organisationnelles

La protection des données personnelles est une priorité absolue pour OFISA Informatique SA (OI). Ce document présente les engagements d'OI en tant que sous-traitant et plus particulièrement les mesures qu'elle met en œuvre pour assurer la sécurité des données personnelles. Il résume de manière transparente ce qu'OI a mis en place pour respecter ses obligations légales, en particulier la Loi fédérale sur la protection des données (LPD).

Rôle d'OI :

La législation fait la différence entre les rôles de responsable du traitement et de sous-traitant. En tant que prestataire informatique, **OI agit en principe en qualité de sous-traitant**. Autrement dit, nous traitons les données personnelles transmises par nos clients uniquement sur instructions et pour le compte de ceux-ci, dans le cadre du contrat.

Rôle du client (responsable du traitement)	**Rôle d'OI** (sous-traitant)
Il est le seul responsable de la manière dont il traite les données personnelles et de sa conformité à la législation applicable. Par conséquent, le client doit mettre en place ses propres mesures, notamment en matière de sécurité des données, afin de respecter ses obligations.	Nous nous engageons à mettre en place des mesures techniques et organisationnelles appropriées, afin de garantir la sécurité de vos données lorsque nous les traitons. En tant que partenaire de confiance, nous assistons et accompagnons également nos clients dans leur propre conformité.

En tant que sous-traitant, OI doit donc assurer l'intégrité et la sécurité de ces données par rapport au risque encouru (art. 8 et 9 LPD), mais les données elles-mêmes restent détenues, gérées et contrôlées par le client. Par conséquent, ce dernier doit prendre des mesures pour respecter ses propres obligations de responsable du traitement. **En tant que partenaire de confiance, nous sommes à la disposition de nos clients pour les assister dans leur conformité et répondre à leurs interrogations.**

Engagements d'OI :

En sa qualité de sous-traitant, OI s'engage à :

1. mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer une sécurité adéquate des données personnelles confiées par ses clients (**sécurité**) ;
2. aider ses clients, dans toute la mesure du possible, à respecter leurs propres obligations, notamment en matière de sécurité des données ou pour répondre à toute demande (**assistance**) ;
3. mettre à la disposition de ses clients, en toute transparence, les informations nécessaires pour démontrer le respect de ses obligations (**transparence**).

Vos personnes de contact :

Selon le type de demande, nous vous invitons à contacter les personnes suivantes :

- nos consultant-e-s pour toutes les questions courantes en lien avec les produits et services ;
- notre responsable de la sécurité des systèmes d'information (RSSI) pour les questions techniques ou concernant la sécurité des données (security@o-i.ch);
- notre délégué à la protection des données (DPO) pour des demandes formelles ou réclamations en lien avec la protection des données au sein d'OI (privacy@o-i.ch).

FAQ :

Est-ce que les produits commercialisés par OI respectent la LPD ?

Les produits d'OI disposent de tous les paramètres permettant de respecter la LPD. Il est cependant de la responsabilité de client, en tant que responsable du traitement, d'appliquer des paramètres et règles respectueux de la protection des données. OI accompagne ses clients dans ce processus.

Est-ce que nous stockons les données personnelles en Suisse ?

Oui, nous stockons les données personnelles exclusivement en Suisse. Nos serveurs se situent dans un centre de données Swisscom hautement sécurisé. Vous trouverez davantage d'informations dans la liste de nos sous-traitants ultérieurs.

Notre programme de protection des données

OI a mis en place un système de gestion de la protection des données et de la sécurité de l'information. Ce système de gestion comprend des exigences et mesures documentées visant à intégrer les règles de protection des données dans les processus métiers de l'entreprise.

Si la responsabilité globale de la protection des données est assumée par la Direction d'OI, tous les collaborateurs sont sensibilisés et doivent s'acquitter de leurs tâches conformément aux exigences en matière de protection des données. De plus, plusieurs rôles ont été créés revêtant une importance particulière, dont celui de délégué à la protection des données et de responsable de la sécurité des systèmes d'information. Par ailleurs, un Comité de protection des données a été mis sur pied pour coordonner les différentes mesures.

Mesures techniques et organisationnelles

Vous trouverez ci-dessous les mesures techniques et organisationnelles d'ordre général mises en œuvre par OI **sur ses systèmes** pour assurer la sécurité des données traitées pour le compte du client dans le cadre du contrat (« Données Client »). Ces mesures doivent permettre d'assurer la confidentialité, la disponibilité, l'intégrité et la traçabilité des données. Pour des raisons de sécurité, seul un résumé est fourni ; davantage d'informations concernant les mesures techniques peuvent être obtenues auprès de notre RSSI.

De plus, OI maintient un processus adapté permettant de contrôler régulièrement et, le cas échéant, de renforcer l'efficacité des mesures techniques et organisationnelles, afin de garantir durablement la sécurité adéquate des données personnelles.

OI traite également des données personnelles concernant des collaborateurs et autres auxiliaires du client pour ses propres buts, notamment à des fins de gestion du contrat et de sécurité (voir

déclaration de protection des données). Ces traitements de données ne sont pas soumis aux dispositions sur la sous-traitance, mais OI prend en substance les mesures techniques et organisationnelles décrites ci-dessous dans ces hypothèses également.

Thématiques de sécurité	Mesures mises en œuvre
Organisation de la sécurité de l'information	**Responsabilité de la sécurité**. OI a mis en place un système de gestion de la sécurité de l'information. Elle a chargé un collaborateur de coordonner et contrôler les règles de sécurité, et nommé un Comité de sécurité pour valider les mesures et procédures adéquates. **Gestion des risques**. OI a procédé à une évaluation des risques de sécurité liés au traitement des Données Clients et met en œuvre les mesures techniques et organisationnelles appropriées en conséquence.
Gestion des actifs	**Inventaire des actifs**. OI conserve un inventaire de tous les supports et environnements sur lesquels les collaborateurs sont autorisés à stocker et traiter des Données Client. L'accès à ces inventaires est restreint au personnel autorisé d'OI. **Gestion des actifs** - Tous les actifs informatiques utilisés pour stocker ou accéder à des Données Client sont attribués à un propriétaire qui est responsable de son utilisation. - Les Données Client sont classifiées pour faciliter leur identification et la restriction de l'accès à ces données. En particulier, les environnements autorisés pour leur traitement sont définis et font l'objet des mesures adéquates. - Toutes les Données Client stockées sur des supports sont effacées de manière sécurisée avant qu'ils ne soient réutilisés. Si cela n'est pas faisable techniquement ou s'ils sont obsolètes, les supports sont détruits. - Les documents papier contenant des Données Client sont systématiquement détruits de manière irréversibles à l'aide d'une déchiqueteuse.
Sécurité des ressources humaines	**Confidentialité.** Le personnel d'OI accédant aux Données Client est soumis à une obligation de confidentialité. **Sensibilisation et formation à la sécurité**. OI forme son personnel aux procédures de sécurité applicables et les sensibilise à la sécurité des données. OI informe également son personnel des conséquences possibles d'un manquement aux règles et procédures.
Contrôle des accès	**Politique de contrôle des accès**. OI dispose d'une directive de contrôle des accès et d'une matrice complète des privilèges de chaque collaborateur ayant accès aux Données Client. **Contrôle des accès fondés sur les rôles** - Les droits d'accès sur les systèmes sont structurés en rôles. Le collaborateur se voit attribuer un ou plusieurs rôles nécessaires à l'exécution de sa fonction. Les rôles sont structurés de sorte que seules les Données Clients nécessaires pour accomplir la tâche peuvent être accessibles. - Les privilèges liés à un nouveau rôle doivent être autorisés par le supérieur du collaborateur et sont mis en œuvre techniquement par le service désigné. Les tâches d'octroi des privilèges et de mise en œuvre techniques des changements sont donc strictement séparées. - La description des rôles et de leurs privilèges est documentée dans la matrice des accès. Cette matrice est régulièrement revue et mise à jour. Pour tous les

Thématiques de sécurité	Mesures mises en œuvre
	rôles, une vérification régulière est effectuée pour savoir si les utilisateurs ont toujours besoin des rôles qui leur sont attribués. - Les droits d'accès des personnes qui cessent leurs activités chez OI ou change de fonction sont immédiatement modifiés, respectivement supprimés. - Lorsque plusieurs de ses collaborateurs sont autorisés à accéder à des systèmes contenant des Données Client, OI veille à ce que chacun utilise des identifiants qu lui sont propres, ou que leurs actions puissent être retracées autrement. **Authentification** - OI applique des procédures conformes aux normes de l'industrie pour identifier et authentifier les utilisateurs tentant d'accéder à ses systèmes informatiques. L'accès des collaborateurs aux systèmes d'OI s'effectue toujours avec leurs identifiants personnels. - L'accès aux systèmes est toujours protégé par au moins un mot de passe ou un élément d'authentification équivalent. Les mots de passe doivent répondre à des exigences minimales de complexité. Les mots de passe des comptes personnels ne seront jamais mis à la disposition de tiers. - Tous les utilisateurs bénéficiant d'un accès distant aux systèmes d'OI doivent se connecter par un tunnel VPN SSL et être authentifiés par un mécanisme d'authentification à double facteurs - OI contrôle les tentatives répétées d'accès à ses systèmes d'information avec un mot de passe non valable. En cas de connexion incorrecte, l'identifiant est temporairement bloqué. - L'accès aux systèmes d'OI depuis un ordinateur privé est strictement interdit et fait l'objet de mesures de blocage. Seuls les ordinateurs professionnels dûment autorisés peuvent accéder au réseau. - L'accès avec des droits administrateurs aux systèmes d'OI se fait toujours par l'intermédiaire d'identifiants dédiés. OI peut déterminer à tout moment quel utilisateur a utilisé le compte administrateur. - Les accès aux systèmes sont enregistrés et analysés par diverses procédures et font l'objet d'une vérification en cas d'incident de sécurité. Les incidents identifiés sont analysés par les responsables désignés et les mesures appropriées sont prises. **Intégrité des identifiants** - OI utilise un outil sécurisé de stockage des mots de passe qui les rend illisibles et auquel l'accès est restreint par une authentification supplémentaire à double facteurs. - OI applique des procédures et mesures pour préserver la confidentialité et l'intégrité des mots de passe lors de leur attribution et distribution, puis de leur stockage. - Les identifiants et mots de passe fournis par des clients doivent être transférés uniquement à l'aide de l'outil de transfert autorisé. **Chiffrement des données au repos**. Les supports et appareils mobiles traitant des Données Client sont chiffrés selon l'état actuel de la technique.

Thématiques de sécurité	Mesures mises en œuvre
Sécurité physique et environnementale	**Localisation des serveurs.** Les serveurs d'OI sur lesquels sont stockés les Données Client se trouvent dans un centre de données Swisscom hautement sécurisé. Les locaux d'OI sont uniquement un point d'accès. **Sécurité physique du centre de données** - Les centres de données de Swisscom sont classés comme zones hautement sécurisées et disposent de mesures de protection physique nécessaires pour détecter rapidement une violation du périmètre du bâtiment et pour réduire autant que possible les risques de phénomènes naturels de telle sorte qu'ils n'aient d'impact sur le fonctionnement des centres. Les pièces hautement sécurisées sont équipées de systèmes d'alarme incendie et de détection de fumée. - Le stockage permanent dans les centres de données est protégé contre les pertes par des mesures de protection physique, comprenant des alimentations électriques redondantes et les systèmes nécessaires pour permettre un fonctionnement autonome pendant une durée limitée. **Sécurité physique des locaux d'OI** - OI restreint l'accès aux locaux qui contiennent des systèmes informatiques traitant des Données Client aux seuls membres autorisés de son personnel. Les visiteurs doivent s'enregistrer et sont accompagnés dans les zones sécurisées par les employés responsables.
Sécurité des communications	**Canaux de communication** - En présence de données sensibles et confidentielles, les Données Client transitant sur les réseaux d'OI sont uniquement importées ou exportées par des canaux de communication chiffrés. - Des mesures de protection de la messagerie et des règles en matière de moyens de communication sont appliquées, afin de protéger les systèmes d'OI. **Sécurité des réseaux** - Les équipements connectés au réseau accessibles depuis des sites distants sont protégés par des règles de filtrage et des politiques de pare-feu restrictives, ainsi que des segmentations VLAN sont mises en œuvre. - La disponibilité des services de réseau est assurée en dupliquant les appareils critiques.
Sécurité des opérations	**Sauvegardes** - Des copies des environnements d'OI contenant des Données Client sont effectués à intervalles réguliers selon la stratégie de sauvegarde, afin d'être en mesure de restaurer ces données. - Les copies sont stockées dans un lieu distinct de celui renfermant les équipements informatiques principaux qui traitent les Données Client. - Des procédures spécifiques régissent l'accès aux copies, lesquelles sont chiffrées selon l'état actuel de la technique. - Les copies de sauvegarde et le processus de leur restauration sont testés au moins une fois par trimestre en remontant les sauvegardes sur les systèmes concernés et en vérifiant que toutes les données ont été récupérées avec succès.

Thématiques de sécurité	Mesures mises en œuvre
	Séparation des données et des environnements. Les environnements de test, développement et production sur lesquels sont stockées et traitées les Données Client sont séparés. **Sécurité des postes de travail**. Les postes de travail utilisés pour accéder à l'environnement de production d'OI et aux Données Client sont gérés de manière centralisée, disposent des correctifs de sécurité applicables, exécutent des logiciels de sécurité standardisés et sont régulièrement analysés pour détecter les vulnérabilités. **Protection contre les logiciels malveillants.** OI a mis en place des mesures de lutte contre les logiciels malveillants afin de protéger les Données Client contre les tentatives d'accès non autorisées. **Journalisation des événements**. OI consigne les accès et utilisations des systèmes informatiques contenant des Données Client, en enregistrant les identifiants d'accès, leurs heures et dates d'accès, les autorisations/refus d'accès et les activités effectuées, afin de garantir la traçabilité des données et de disposer de preuves si nécessaire.
Gestion des incidents de sécurité informatique	**Procédure de gestion des incidents** - OI conserve un registre des incidents de sécurité décrivant les failles, la période concernée, les causes, les conséquences, ainsi que la procédure de récupération de données appliquée. Les vulnérabilités sont également journalisées à des fins de suivi et de correction. - Pour chaque incident de sécurité qui est une violation de données, une notification sera envoyée par OI sans délai au client, conformément à la Loi fédérale sur la protection des données. **Surveillance des vulnérabilités et incidents**. Les collaborateurs désignés par OI procèdent à une analyse détaillée du registre et journal au moins tous les trois mois afin d'identifier les évènements récurrents et de proposer des mesures correctives.
Gestion de la continuité des opérations	**Stratégie de continuité** - OI dispose de plans de secours et de reprise d'activité pour les systèmes informatiques traitant des Données Client. - Les systèmes de stockage redondants et les procédures de récupération de données d'OI sont conçus pour restaurer les Données Client dans l'état d'origine ou précédant leur perte ou destruction.
Contrôle des fournisseurs	**Fournisseurs** - OI sélectionne les éventuels sous-traitants ayant accès aux Données Clients conformément aux règles légales et transfère les responsabilités pertinentes relatives à la protection des données et à la confidentialité au fournisseur.
Contrôle et gestion du changement	**Gestion du changement.** Sur la base d'une analyse des risques, les nouveaux services et changements apportés aux systèmes font l'objet d'un examen technique. Les mesures adéquates sont appliquées avant toute mise en œuvre effective du changement ou du nouveau service. **Audit interne.** OI effectue régulièrement des audits des systèmes. Au niveau technique, il s'agit d'un contrôle régulier de la mise en œuvre et du respect des mesures de protection de base sur les systèmes, conformément aux exigences internes.

Dernière mise à jour : 18 décembre 2023