Accord de traitement des données
Annexe 1 : **Concept de protection des données**

Version : 2.5. 17.08.2023
Contact : Matthias Menne, Délégué à la protection des données, onOffice GmbH

Introduction

L'annexe 1 décrit les mesures techniques et organisationnelles conformément à l'article 32 du RGPD, destinées à garantir la sécurité des traitements couverts par le contrat :

- Mise à disposition de la solution logicielle CRM en ligne onOffice enterprise
- Hébergement de sites web
- Importation de données
- Transferts de données
- Hébergement de courriels

La plupart de ces traitements sont effectués sur les mêmes systèmes informatiques et avec les mêmes mesures de sécurité. Ainsi, au début de chaque chapitre, ces mesures de sécurité communes sont décrites, suivies des détails spécifiques à chaque traitement.

Cryptage

Le trafic réseau entrant et sortant d'onOffice enterprise est sécurisé par HTTPS. Les versions TLS 1.0, 1.1 et 1.2 sont prises en charge. Le certificat a été émis par « GMO GlobalSign Inc », Portsmouth NH, USA.

Les sites web peuvent être sécurisés par des certificats vérifiés par l'autorité de certification « Let's Encrypt », San Francisco CA, USA. Les supports de données envoyés dans le cadre des importations de données sont cryptés avant d'être renvoyés au client.

Lors de l'envoi de courriels, TLS avec Perfect Forward Security est utilisé, dans la mesure où le serveur de réception le supporte.

Confidentialité

La confidentialité des données personnelles est assurée par le fait que seules les personnes autorisées ont un accès physique ou logique à ces données.

Contrôle d'accès physique

Sauf indication contraire, tous les traitements ont lieu dans le centre de données de Telehouse Deutschland GmbH (voir annexe 2). Un système de carte sans contact, une surveillance 24/7 par des gardes de sécurité et une surveillance vidéo assurent le contrôle d'accès.

Les droits d'accès aux salles de serveurs sont programmés spécifiquement pour chaque salle.
Les sauvegardes sont stockées dans des locaux loués à Equinix (Germany) GmbH à Düsseldorf. Les employés des deux centres de données n'ont pas accès aux données stockées.

Dans les bureaux de la société onOffice GmbH à Aix-la-Chapelle, les données personnelles du client ne sont stockées que temporairement, soit pour des tests logiciels internes, soit pour des importations de données, lorsque cela est absolument nécessaire. La distribution des clés aux employés est réglementée et documentée. En dehors des heures de travail, les bureaux sont protégés par un système d'alarme qui, en cas de déclenchement, alerte automatiquement une société de sécurité.

Les supports de données envoyés dans le cadre des importations de données sont conservés en toute sécurité dans les locaux de l'entreprise. Leur traçabilité est documentée par écrit. Les importations de données sont effectuées sur un serveur dédié situé dans un espace sécurisé au sein des locaux d'onOffice GmbH à Aix-la-Chapelle, protégé par une alarme, un enregistrement des accès et une surveillance vidéo.

Contrôle d'accès utilisateur

L'accès à onOffice enterprise n'est possible qu'avec la saisie correcte du nom du client, du nom d'un utilisateur actif non bloqué et d'un mot de passe valide. Le nom d'utilisateur et le mot de passe ne sont pas affichés en clair lors de la saisie. La fréquence de modification des mots de passe peut être définie par un administrateur via le logiciel. La complexité des mots de passe est automatiquement vérifiée lors de la saisie ; si elle ne répond pas aux critères définis, le mot de passe est rejeté.

L'accès aux systèmes de production est restreint à un nombre minimal de personnes et est sécurisé par une authentification Public-Private-Key. Lorsque des employés quittent onOffice, leurs accès sont supprimés.

Les logiciels standards installés sur les serveurs sont régulièrement vérifiés pour les mises à jour critiques de sécurité, qui sont installées aussi rapidement que possible sans compromettre la disponibilité.

Les données personnelles des clients ne sont traitées par les employés d'onOffice GmbH en dehors des locaux de l'entreprise que si nécessaire. La politique de sécurité informatique est respectée dans ces cas, de la même manière que dans les locaux de l'entreprise. Le trafic réseau est surveillé par un pare-feu matériel.

Contrôle d'accès aux données

Dans onOffice enterprise, l'accès aux enregistrements de données peut être limité par utilisateur. Pour cela, les enregistrements doivent être attribués à des utilisateurs ou à des groupes spécifiques, et les droits des utilisateurs doivent être restreints en conséquence. Un module supplémentaire permet de définir les droits de lecture et d'écriture pour chaque utilisateur sur les enregistrements d'adresses, d'objets ou d'historiques individuels. Les utilisateurs peuvent créer une liste des derniers enregistrements qu'ils ont ouverts.

Les boîtes aux lettres électroniques dans onOffice enterprise peuvent être attribuées à un ou plusieurs utilisateurs, de sorte que la boîte de réception ne soit plus accessible à d'autres utilisateurs.

Intégrité

Toutes les modifications apportées aux données d'adresses et d'objets dans onOffice enterprise sont enregistrées et peuvent être consultées par les utilisateurs ayant des droits d'administrateur. onOffice enterprise est conçu pour être multi-locataires, chaque client ayant sa propre base de données. Il est impossible pour un utilisateur de consulter les données d'autres clients sans se connecter à leur version avec le nom du client, l'utilisateur et le mot de passe appropriés.

Les modifications du code source d'onOffice enterprise sont soigneusement testées et mises à disposition pendant plusieurs semaines à un groupe limité de clients avant d'être déployées pour tous. Les correctifs sont appliqués deux fois par semaine pour tous les clients, et immédiatement en cas d'urgence.

Les pièces jointes aux courriels sont vérifiées pour les virus, et une protection antivirus est en place ou en cours de déploiement pour les autres traitements.

Disponibilité

Les bases de données des clients sont sauvegardées chaque nuit par une sauvegarde complète. Ces sauvegardes sont stockées dans les locaux loués par Telehouse Deutschland GmbH au centre de données d'Equinix à Düsseldorf (voir annexe 2). Les fichiers des clients sont sauvegardés une fois par mois par une sauvegarde complète et chaque nuit par une sauvegarde incrémentielle.

Sauf pour les « Importations de données » et les « Transferts de données », tous les traitements sont effectués dans le centre de données de Telehouse. La disponibilité des données est garantie par une alimentation de secours redondante N+1, une protection contre les incendies avec des détecteurs de chaleur et de fumée optiques/thermiques, des systèmes d'extinction au gaz inerte Inergen, ainsi que des connexions réseau redondantes à plusieurs opérateurs. Des ressources informatiques suffisantes sont disponibles pour compenser la panne de plusieurs serveurs. Les données des clients sont stockées dans un système RAID5.

Pour se protéger contre les attaques DDoS, onOffice participe au réseau Prolexic d'Akamai. Toutes les demandes adressées aux systèmes d'onOffice GmbH sont acheminées via les serveurs d'Akamai, qui filtrent les requêtes faisant partie d'une attaque DDoS.

Légalité du traitement

Tous les employés d'onOffice GmbH sont soumis à une obligation de confidentialité et reçoivent une formation sur la protection des données et la sécurité informatique. Des accords de traitement des données ont été signés avec tous les sous-traitants. Ces sous-traitants sont évalués avant la signature du contrat pour s'assurer que leurs employés sont également tenus au secret.

Le principe de minimisation des données est intégré dans la planification des fonctionnalités et des processus (« Privacy by Design »).

Gestion de la protection des données

Le concept de protection des données est mis en œuvre à travers des procédures, des accords et des mesures techniques et organisationnelles. L'adéquation du concept est vérifiée au moins une fois par an. Si nécessaire, le concept ou sa mise en œuvre est ajusté.

Gestion des incidents

Les systèmes informatiques utilisés pour les traitements sont surveillés en permanence. En cas d'incident, l'accès aux données personnelles est rétabli le plus rapidement possible. Après un incident, une analyse est effectuée pour déterminer si des ajustements doivent être apportés au concept de sécurité informatique ou au plan d'urgence informatique, et si les mesures techniques et organisationnelles et l'infrastructure informatique sont suffisantes pour éviter qu'un incident similaire ne se reproduise.

Traitement des données dans des pays tiers

OnOffice utilise le réseau Prolexic d'Akamai. Pour garantir une protection optimale contre les attaques DDoS, le trafic vers les systèmes d'onOffice GmbH est acheminé via des serveurs situés dans le monde entier. La surveillance du trafic est effectuée aux États-Unis. Par conséquent, les données personnelles suivantes peuvent être traitées en dehors de l'UE :

1. l'adresse IP du client,
2. le domaine demandé,
3. en l'absence de cryptage HTTPS : l'URL.

onOffice a conclu avec Akamai les clauses contractuelles types de l'UE de juin 2021, en utilisant le module 3 (processeur et processeur).

Une analyse de la législation américaine et une évaluation des risques ont été effectuées. Aucune autre mesure de sécurité supplémentaire n'est nécessaire.