Mesures techniques et organisationnelles conformément à l'art. 32 du RGPD

Informations sur le document	
Version	1.0
Date	7.2.2019
Classification du document	Public
Statut de validation	Approuvé
Version originale publiée par	Délégué à la protection des données 1&1
Version actuelle publiée par	Délégué à la protection des données du groupe United Internet AG
Publié le	7.2.2019

Remarque

Ce document contient des informations qui sont mises à la disposition des partenaires commerciaux, des clients et d'autres parties externes qui disposent d'un droit de regard légal ou justifié.

Pour des raisons de lisibilité, la forme masculine a été choisie dans ce document, mais ce dernier concerne en réalité tous les sexes.

Préambule

L'entité responsable a mis en œuvre des mesures appropriées en matière de confidentialité, d'intégrité, de disponibilité et de fiabilité, ainsi que des procédures régulières d'examen, d'évaluation et d'appréciation.

La partie générale décrit les mesures techniques et organisationnelles qui s'appliquent à tous les services, lieux et clients. Les annexes décrivent les mesures qui s'appliquent au-delà de celles qui sont documentées dans la partie générale.

1. Confidentialité

Des données personnelles sont dites confidentielles lorsqu'elles ne sont pas rendues disponibles ou divulguées à des personnes, entités ou processus non autorisés.

Contrôle des entrées

- Service d'accueil et de sécurité
- Autorisations d'accès individuelles, documentées et différentes selon le rôle (cartes, transpondeurs et clés)
- Laissez-passer pour les employés et les visiteurs
- Les visiteurs ne sont autorisés à rester dans le bâtiment que s'ils sont accompagnés d'un employé
- Système d'alarme en cas de cambriolage/effraction extérieure
- Les bureaux sont fermés à clé en dehors des heures de travail

Contrôle des accès aux systèmes

- Procédures formelles d'utilisation et d'autorisation
- Connexion uniquement avec un nom d'utilisateur, un mot de passe et, le cas échéant, une authentification à deux facteurs
- Politiques de mots de passe systématiquement appliquées
- VPN pour les accès à distance et à travers des dispositifs gérés par le responsable
- Gestion des appareils mobiles
- Les supports de données mobiles sont cryptés
- Verrouillage automatique des postes de travail après quelques minutes d'inactivité
- Politique de bureau propre

Contrôle des accès aux données

- Tenue de registres des actifs et élaboration de mesures sur la base de la classification des données
- Utilisation de procédures de chiffrement (p. ex. cryptage)
- Mise en œuvre des concepts d'autorisation selon le principe du "need-to-know"
- Séparation entre les accès aux applications et les accès à l'administration des applications
- Enregistrement des tentatives d'accès
- Configuration des postes de travail des administrateurs
- Nombre minimum défini d'administrateurs
- Destruction des documents jetés

Pseudonymisation

- Dans la mesure du possible ou si nécessaire, les données personnelles seront traitées avec un pseudonyme (séparation des données d'attribution et stockage dans un système séparé)

Contrôle par séparation

- Séparation de l'environnement de développement, de test et de production
- Les données personnelles ne peuvent pas être utilisées à des fins de test
- Multi-tenancy / séparation logique des données dans les applications concernées : bases de données séparées, séparation des schémas dans les bases de données, concepts d'autorisation et/ou stockage structuré des fichiers

2. Intégrité

L'intégrité des données personnelles est préservée si elles sont exactes, inchangées et complètes.

Contrôle des transferts

- Mise à disposition de données via des connexions cryptées (par ex. SFTP)
- Divulgation de données à caractère personnel selon le principe "Need-to-Know ou "Need-to-Do"
- Les données personnelles sont classées en fonction de leur besoin de protection, les données confidentielles ne pouvant être transmises que par des voies de communication sécurisées
- Le chiffrement des emails est utilisé dans la mesure du possible
- Dans la mesure du possible, les données personnelles ne sont transmises que sous forme anonyme ou avec un pseudonyme
- Documentation de la distribution des supports de stockage physiques
- Divulgation de documents papier contenant des données à caractère personnel dans une enveloppe opaque scellée

Contrôle des saisies

- Enregistrement technique de la saisie, de la modification et de l'effacement des données personnelles et contrôle des enregistrements
- Traçabilité de la saisie, de la modification et de la suppression des données via des noms d'utilisateur individuels (et non via des groupes d'utilisateurs)
- Concept d'autorisation basé sur les rôles (droits de lecture, d'écriture et de suppression)
- Enregistrement des modifications administratives

3. Disponibilité et fiabilité

La disponibilité des données personnelles est assurée si elles peuvent toujours être utilisées comme prévu par les utilisateurs

- Utilisation de pare-feu matériels et logiciels
- Systèmes de détection d'intrusion
- Protection contre les surtensions de l'enveloppe extérieure du bâtiment contre la foudre
- Alimentation sans interruption
- Manuels d'urgence pour la récupération des données, la protection contre la destruction accidentelle et la perte
- Réalisation de tests de récupération
- Si nécessaire, utilisation de systèmes redondants (par ex. RAID)
- Tests réguliers des sauvegardes de données
- Audits externes et tests de sécurité

4. Procédures régulières d'examen, d'évaluation et d'appréciation

Comment s'assure-t-on que les mesures de protection des données mentionnées sont régulièrement réexaminées ?

Gestion de la protection des données

- Des responsables de la protection des données et un responsable de la sécurité de l'information sont nommés
- Mise en place d'une organisation de protection des données et de sécurité de l'information
- Tous les employés sont tenus à la confidentialité lors du traitement des données personnelles et sont informés du secret des télécommunications
- Les employés sont sensibilisés au traitement des données personnelles
- Les nouveaux employés reçoivent du matériel d'information sur le traitement des données personnelles
- Un registre des activités de traitement est tenu à jour et des évaluations sur la protection des données sont effectuées si besoin
- Des processus pour l'exercice des droits des personnes concernées ont été mis en place

Contrôle des commandes

- Les données traitées pour le compte du client ne sont traitées que selon les instructions du client
- Les mandataires sont soigneusement sélectionnés en fonction des mesures techniques et organisationnelles prises pour protéger les données à caractère personnel
- Les instructions relatives au traitement des données personnelles sont documentées sous forme de texte
- Le cas échéant, des accords de traitement ou des garanties appropriées pour le transfert de données vers des pays tiers sont conclus

Réglages par défaut respectant la vie privée

- Il est garanti que les systèmes et les produits sont développés dans le respect de la protection des données
- Seules les données personnelles nécessaires à la réalisation de l'objectif visé sont collectées

Gestion des interventions en cas d'incident

- Processus documenté de détection, de déclaration et de documentation des atteintes à la protection des données avec la participation du responsable de la protection des données
- Procédure documentée du traitement des incidents de sécurité avec la participation du responsable de la sécurité de l'information

Annexe 1 : Mesures techniques et organisationnelles spécifiques pour les centres de calcul

- Tous les centres de calcul sont certifiés selon la norme ISO 27001
- Les systèmes électroniques de contrôle d'accès surveillent et garantissent l'accès au centre de calcul correspondant uniquement aux personnes autorisées
- Portail de sécurité
- Des caméras vidéo ainsi que des détecteurs de cambrioleurs surveillent l'enveloppe extérieure du bâtiment
- Zones de sécurité définies
- Infrastructure réseau hautement redondante
- Le détecteur d'incendie et/ou de fumée est directement relié aux pompiers locaux
- Système de refroidissement dans le centre de calcul / salle des serveurs
- Surveillance de la température et de l'humidité de la salle des serveurs
- Pas de connexions sanitaires dans ou au-dessus des centres de calcul
- Message d'alarme en cas d'accès non autorisé aux centres de calcul