Security Policy

Mesures de sécurité techniques et organisationnelles
Axess s'engage – et engage le centre de données externe dans le cadre de son contrat avec ce dernier – à se conformer aux exigences particulières en matière de protection des données. Les centres de données aussi bien internes qu'externes se trouvent en Autriche. Dans ce contexte, la société Axess AG s'efforce en continu de prendre toutes les mesures nécessaires pour assurer le traitement des données fournies sur les installations de traitement de données conformément au Règlement général sur la protection des données (RGPD) lors de l'exécution de l'ordre ainsi que de concevoir l'organisation interne de l'entreprise de manière à ce que les exigences particulières en matière de protection des données soient remplies.

Il est fait en sorte que les zones de sécurité, le cercle de personnes autorisées et les autorisations d'accès soient désignés de manière fixe, que les voies ou moyens d'accès soient sécurisés en conséquence et que les supports de données soient contrôlés et conservés de manière sécurisée.

À cet égard, il s'agit en particulier actuellement des mesures requises suivantes:

1. Contrôle des entrées
L'accès physique aux installations de traitement de données à l'aide desquelles des données sont traitées ou utilisées est interdit aux personnes non autorisées. Les salles informatiques se trouvent à l'intérieur d'un bâtiment de bureaux classé comme résistant aux séismes et situé dans une zone mixte. Le contrôle des entrées – uniquement collaborateurs du département informatique (IT), du département de gestion des installations et membres de la direction – est garanti par les mesures suivantes:
> Carte de légitimation/carte à puce
Toute présence dans la zone de sécurité est enregistrée. Le personnel non autorisé et les personnes étrangères à l'entreprise (techniciens du service de maintenance, conseillers, personnel de nettoyage, etc.) n'ont le droit de pénétrer dans les locaux que s'ils sont accompagnés par des personnes autorisées. Le contrôle des entrées est renforcé par les mesures organisationnelles/techniques complémentaires suivantes:
> Système d'alarme
> Surveillance du bâtiment
> Équipement vidéo

2. Contrôle de l'accès aux données
L'utilisation des systèmes de traitement de données par des personnes non autorisées est empêchée à l'aide des mesures suivantes:
> Mot de passe
Chaque personne autorisée possède son propre mot de passe connu d'elle seule et devant être modifié à intervalles réguliers. Des protocoles automatiques (fichiers log) sont établis concernant l'intégralité des activités sur les installations de traitement de données et de télécommunication. L'utilisation de systèmes de traitement de données par des personnes non autorisées au moyen de dispositifs de transfert de données est empêchée à l'aide des mesures suivantes:
> VPN (Virtual Private Network)

3. Contrôle des interventions
Il est garanti que les personnes autorisées à utiliser un système de traitement de données ne peuvent recourir qu'aux données correspondant à leur autorisation respective, et que les données ne peuvent être ni lues, ni copiées, ni modifiées, ni supprimées de manière non autorisée lors du traitement, de l'utilisation ou de l'enregistrement. La limitation des possibilités d'intervention et de recours de la personne autorisée aux seules données correspondant à son autorisation respective est garantie à l'aide des mesures suivantes:
> Contrôle automatique de l'autorisation d'intervention (dans le système)

4. Contrôle de l'usage prévu
Il est garanti, à l'aide des mesures suivantes, que les données collectées à des fins différentes sont traitées de manière séparée les unes des autres:
> Sur base logicielle (par ex. séparation des clients)
> Séparation via la réglementation des accès et interventions (selon le principe des banques de données)
> Séparation des données d'essai et des données actuelles
> Séparation des systèmes d'essai et des systèmes actuels (matériel technique, programmes)

5. Pseudonymisation
Dans la mesure où c'est possible pour le traitement des données en question, nous éliminerons les caractéristiques d'identification primaires des données personnelles dans les différentes applications de données et nous les conserverons séparément.

6. Contrôle des transmissions
Il est garanti que les données à caractère personnel ne peuvent être ni lues, ni copiées, ni modifiées, ni supprimées de manière non autorisée lors de leur transmission électronique ou durant leur transport ou leur enregistrement sur des supports de données, et qu'il est possible de vérifier et de constater à destination de quels services est prévue une transmission de données à caractère personnel par des dispositifs de transmission de données. L'envoi de supports de données est documenté et contrôlé par un enregistrement et une fiche d'accompagnement. Il est interdit d'apporter et d'utiliser des supports de données privés. Les supports de données sont détruits de la manière suivante:
> Supports de données magnétiques: par écrasement des données et destruction physique (prestataire de services externe)

Dans la mesure où Internet est utilisé pour la transmission de données à caractère personnel, les mesures de sécurité suivantes sont appliquées:
> Pare-feu
> Virtual Private Network (VPN)

7. Contrôle des saisies
Il est garanti qu'il est possible de vérifier et de constater ultérieurement si – et par qui – des données à caractère personnel ont été saisies, modifiées ou supprimées dans des systèmes de traitement de données. Pour cela, le prestataire documentera et enregistrera les saisies.

8. Contrôle de la disponibilité
Il est garanti, à l'aide des mesures suivantes, que les données à caractère personnel sont protégées contre toute destruction ou perte aléatoire:
> Sauvegarde de données quotidienne/hebdomadaire/mensuelle/annuelle
> Storage Areal Network (SAN)
> Duplication de disques (RAID, etc.)
> Alimentation sans interruption (ASI)
> Filtre de surtension
> Générateurs de secours
> Externalisation de données
> Dispositifs de protection anti-incendie

9. Gestion de la protection des données
On s'assurera qu'une gestion de la protection des données sera mise en place et appliquée. La gestion de la protection des données est composée des points suivants:
> Registre des traitements
> Traitement des données de commande
> Évaluation des conséquences de la protection des données
> Incident-Response-Management (plan de réponse aux incidents)
> Signalisation des atteintes à la protection des données
> Formations
> PDCA (Plan, Do, Check, Act; prévoir, faire, contrôler, agir): contrôles réguliers

10. Incident-Response-Management
Des mesures ont été prises sur la manière dont les personnes compétentes doivent réagir en fonction des scénarios potentiels. Parmi ceux-ci on compte les manquements à la sécurité des données, le déni de service (Denial of Service, DoS), le déni de service distribué (Distributed Denial of Service, DDoS), les lacunes dans le pare-feu, les irruptions de virus ou de logiciels malveillants ainsi que les menaces venant de l'intérieur.
Le plan de réponse aux incidents est composé de six phases importantes:
> Identification: Aussi bien l'utilisateur que le collaborateur du service informatique sont formés ou informés de l'apparition possible d'incidents et des démarches à entreprendre.
> Identification: Déterminer qu'il s'agit bien d'un incident de protection des données dans le cas de l'événement.
> Endiguement: Limiter les dégâts engendrés par l'incident et isoler les systèmes touchés pour éviter d'autres dommages.
> Éradication: Trouver l'origine ou la cause de l'incident et retirer les systèmes touchés de l'environnement productif.
> Restauration: Réintégrer les systèmes touchés dans l'environnement productif après s'être assuré qu'il n'y a plus d'autre menace.
> Informations recueillies: Compléter la documentation de l'incident et réaliser une analyse pour permettre à l'équipe ou à l'entreprise d'en tirer un apprentissage. On peut de cette manière éventuellement améliorer les réactions futures.

11. Privacy by Design & Privacy by Default
On s'est assuré d'avoir pris des mesures techniques et organisationnelles adaptées pour garantir que d'une manière générale seules des données personnelles sont traitées grâce aux paramétrages par défaut correspondants et que ce traitement est nécessaire pour l'objectif défini en question:
> Les données personnelles ne sont collectées que si elles sont nécessaires à l'exécution du contrat (cartes saisonnières, etc.)
> L'implantation de cookies dans les boutiques en ligne n'est possible qu'avec l'autorisation de l'utilisateur
> L'utilisation des données personnelles à des fins de marketing n'est permise qu'avec l'autorisation active de l'utilisateur

Security Policy

12. Contrôle des ordres

Il est garanti que les données à caractère personnel traitées pour le compte de tiers sont uniquement traitées conformément aux instructions du donneur d'ordre. Il existe des contrats pour les types suivants de traitement de données sur commande:

> Traitement de données par des prestataires externes
> Destruction de supports de données/Élimination par des prestataires externes
> Maintenance et télémaintenance par des prestataires externes
> Administration/télé-administration par des prestataires externes

Le traitement de données à caractère personnel sur commande – uniquement selon les instructions du donneur d'ordre – est garanti par les mesures suivantes:

> Instructions écrites
> Offre et confirmation d'ordre
> Pseudonymisation

13. Sous-traitant des commandes

> CN Group CZ s.r.o.
> Agence LOOP New Media GmbH
> conova communications GmbH