Politique de sécurité

1 Préambule

L'objet, l'ampleur, la nature et la finalité du traitement des données découlent de la relation commerciale basée sur le contrat de vente conclu entre les parties et remplacent tous les accords antérieurs à ce sujet. Les présentes mesures de sécurité complètent le contrat de vente conclu entre le client et Axess, dans la mesure où il se rapporte au traitement des données du client, et sont considérées comme faisant partie intégrante de ce contrat. Axess garantit les mesures de sécurité informatique suivantes dans le cadre de sa relation avec ses clients.

2 Mesures techniques et organisationnelles générales

Axess prend toujours toutes les mesures nécessaires pour le traitement des données transmises dans les systèmes de traitement des données, conformément au RGPD, et garantit que l'organisation interne est conçue de manière à répondre aux exigences de la protection des données. Les dispositions suivantes s'appliquent indépendamment du lieu d'hébergement du serveur.

2.1 Contrôle de l'utilisation prévue :

Les mesures suivantes garantissent que les données collectées à des fins différentes sont traitées séparément :

> Basées sur un logiciel (séparation des clients, par exemple)
> Séparation par un contrôle de l'accès (principe de la base de données)
> Séparation des données de test et actuelles
> Séparation des systèmes de test et des systèmes en service (technique, programmes)

2.2 Pseudonymisation

Dans la mesure où cela 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 sauvegardons séparément.

2.3 Contrôle de la saisie :

Il est assuré qu'il est possible de vérifier et de déterminer ultérieurement si et par qui des données à caractère personnel ont été introduites et modifiées dans les systèmes de traitement des données ou supprimées de ces systèmes. Dans cet objectif, Axess documente ou enregistre les entrées/fichiers journaux.

2.4 Privacy by Design & Privacy by Default

Les paramètres par défaut définis dans le cadre des mesures techniques et organisationnelles garantissent que seules les données à caractère personnel dont le traitement est nécessaire à la finalité du traitement indiquée sont traitées.

> Les données personnelles ne sont collectées que si elles sont nécessaires à l'exécution du contrat de vente (cartes d'abonnement, etc., par exemple).
> L'implantation de cookies dans les boutiques en ligne d'Axess 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

3 Mesures techniques et organisationnelles de l'hébergement de serveurs par Axess

Si les prestations de service DATA CENTER SERVICE sont commandées dans le cadre du contrat de vente, il est garanti que les zones de sécurité et le groupe de personnes autorisées ou les autorisations d'accès sont définis, que les voies d'accès sont sécurisées en conséquence et que les supports de données sont contrôlés et conservés de manière sécurisée. Les mesures suivantes ne s'appliquent que si le serveur est hébergé par Axess.

3.1 Contrôle de l'accès :

L'accès aux installations dans lesquelles les données sont traitées est interdit aux personnes non autorisées. Les salles informatiques sont situées dans un immeuble de bureaux qui a été classé comme résistant aux tremblements de terre. Seuls les collaborateurs des services informatiques et immobiliers et de la direction ont accès à ces locaux. Cet accès est contrôlé par la mesure suivante :

> Autorisation/carte à puce

Toute présence dans la zone de sécurité est enregistrée. Le personnel non autorisé et les personnes étrangères à l'entreprise (techniciens de service, conseillers, personnel de nettoyage, etc.) ne peuvent pénétrer dans ces locaux qu'en compagnie de personnes autorisées. Le contrôle d'accès est complété par les autres mesures organisationnelles/techniques suivantes :

> Système d'alarme
> Surveillance de bâtiments
> Technique vidéo

3.2 Contrôle de l'accès :

Les mesures suivantes empêchent l'utilisation des systèmes de traitement des données par des personnes non autorisées :

> Mot de passe

Chaque personne autorisée dispose de son propre mot de passe, connu d'elle seule, qui doit être modifié à intervalles réguliers. Des protocoles automatiques (journaux) sont établis pour toutes les activités sur l'installation de traitement des données et de télécommunication. L'utilisation de systèmes de traitement des données à l'aide de dispositifs de transmission de données par des personnes non autorisées est empêchée par les mesures suivantes :

> VPN (réseau privé virtuel)

3.3 Contrôle de l'accès :

Il est assuré que les personnes autorisées à utiliser un système de traitement de données ne peuvent accéder qu'aux données auxquelles elles ont droit et que les données ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et le stockage. La limitation de l'accès de la personne autorisée aux données soumises exclusivement à son autorisation d'accès est garantie par les mesures suivantes :

> Contrôle automatique des droits d'accès (dans le système)

3.4 Contrôle des transmissions :

Il est assuré que les données à caractère personnel ne peuvent être lues, copiées, modifiées ni supprimées de manière non autorisée lors de leur transmission par voie électronique ou pendant leur transport ou leur stockage sur des supports de données et qu'il est possible de vérifier et d'établir à quel moment une transmission de données à caractère personnel est prévue par les appareils de transmission. L'envoi de supports de données est documenté et contrôlé par des papiers de déclaration et d'accompagnement. Il est interdit d'apporter et d'utiliser des supports de données privés dans ces locaux.
Les supports de données sont détruits de la manière suivante :

> Supports de données magnétiques par écrasement et destruction physique (prestataire de services externe)

Dans la mesure où les données à caractère personnel sont transmises par Internet, les mesures de sécurité suivantes sont employées :

> Pare-feu
> Réseau privé virtuel (VPN)

3.5 Contrôle de la disponibilité :

Les mesures suivantes garantissent que les données à caractère personnel sont protégées contre toute destruction ou perte accidentelle :

> Sauvegarde des données quotidienne/hebdomadaire/mensuelle/annuelle
> Réseau de stockage (SAN)
> Disques en miroir (RAID entre autres)
> Alimentation sans interruption (ASI)
> Filtre de surtension
> Groupe électrogène de secours
> Externalisation des données
> Dispositifs de pare-feu

3.6 Gestion de la protection des données

La mise en place et l'application d'une gestion de la protection des données sont garanties. La gestion de la protection des données est composée des points suivants :

> Registre des activités de traitement
> Traitement des données de commande
> Évaluation des conséquences de la protection des données
> Gestion des réponses aux incidents
> Signalisation des atteintes à la protection des données
> Formations continues
> PDCA (Plan, Do, Check, Act ; prévoir, faire, contrôler, agir) : contrôles réguliers

3.7 Gestion des incidents

Des mesures ont été prises sur la manière dont les personnes responsables doivent réagir en fonction des scénarios possibles. 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 ou les menaces venant de l'intérieur.
La gestion et réponse aux incidents est composée autour de six phases essentielles :

> Préparation : aussi bien l'utilisateur que le collaborateur du service informatique sont informés de l'apparition possible d'incidents et des démarches à entreprendre.
> Identification : déterminer qu'il s'agit d'un incident de protection des données dans le cas de l'événement.
> Limitation : limiter les dommages causés par l'incident et isoler les systèmes concernés afin d'éviter tout autre dommage
> Élimination : déterminer la cause ou le déclencheur de l'incident et retirer les systèmes concernés de l'environnement de production.
> Restauration : réintégrer les systèmes touchés dans l'environnement productif après s'être assuré qu'il n'y a plus d'autre menace.
> Informations : compléter la documentation de l'incident et réaliser une analyse pour permettre à l'équipe ou à l'entreprise d'en tirer un apprentissage. Il est ainsi possible d'améliorer éventuellement les réactions futures.

4 Accès aux données des clients

Afin de pouvoir fournir un support adapté en cas de problèmes, Axess se réserve le droit, en tant que responsable du traitement des données, d'accéder au système ou aux données du client, dans la mesure où un tel accès est couvert par le contrat de vente entre Axess et ce client, si le client a accepté un tel accès, ou si le revendeur a transmis à Axess une demande de service souhaitée au nom du client.

Politique de sécurité

Axess garantit que :
> un accès physique au matériel du centre de données n'a lieu que si le client commande la prestation de services Data Center Service d'Axess ;
> l'accès aux données du client par le biais de l'outil de télémaintenance ne se fait que dans le cas décrit ci-dessus et avec l'accord ou sur ordre du revendeur et/ou du client ;
> L'accès aux appareils locaux n'est accordé qu'en cas d'assistance, à la demande du client ou du revendeur.

5 Traitement des commandes :
En complément de la présente relation commerciale, ces dispositions relatives au traitement des commandes garantissent le respect de toutes les obligations mutuelles conformément au règlement général sur la protection des données (« RGPD »).

Axess traite les données personnelles pour le compte du client, l'objet, l'étendue, le type, les catégories de données traitées, la finalité du traitement ainsi que les catégories de personnes concernées (données clients) découlant du contrat de vente respectif entre les parties contractantes. Ces dispositions relatives au traitement des commandes complètent donc tous les contrats conclus entre le client et Axess, dans la mesure où ils se rapportent au traitement des données à caractère personnel.

Le traitement des données par Axess a lieu exclusivement dans un État membre de l'Union européenne, les traitements de données transfrontaliers devant être communiqués au commanditaire en tant que responsable en temps utile avant le début du traitement, conformément à l'article 4 Z 23 du RGPD (au sein de l'Union), afin que le commanditaire ait la possibilité de s'y opposer. L'absence de réponse à cette communication équivaut à un consentement au traitement.

5.1 Obligations du sous-traitant :
En signant le contrat d'achat, le client accepte les mesures techniques et organisationnelles définies dans la présente politique. Par la mise en œuvre de cette politique et le respect des instructions générales et individuelles du client concernant les données personnelles (par exemple la suppression des données du client, l'anonymisation des données), Axess garantit un niveau de protection des applications de données contractuelles correspondant à l'état actuel de la technique, si bien que des revendications de toute nature ne peuvent être faites qu'en cas de violation.

Les modifications des mesures techniques et organisationnelles qui garantissent le même niveau de protection des données personnelles traitées ou qui l'augmentent sont considérées comme approuvées et sont communiquées au client sur demande, mais Axess n'est cependant pas tenu de les communiquer au client.

Axess prend les mesures techniques et organisationnelles décrites ci-dessus pour que le client puisse exercer ses droits de la personne concernée conformément au chapitre III du RGPD (renseignement, accès, rectification, effacement, limitation, portabilité des données, contestation ainsi que décision individuelle automatisée dans certains cas) dans les délais légaux.

5.2 Traitement de données
Axess s'engage à ne traiter les données personnelles que dans le cadre des contrats existants et selon les instructions individuelles du client. Si Axess est obligé par la loi de transmettre les données à des tiers, il informe le client de son obligation légale de transmettre ses données. Toute autre transmission de données à des fins ne relevant pas de la relation contractuelle n'a lieu que sur instruction du client, sur la base d'un ordre écrit.

Axess s'assure que toutes les personnes chargées du traitement des données sont tenues au secret des données avant le début de leur activité et également après la fin de celle-ci ou sont soumises à une obligation légale de confidentialité équivalente.

5.3 Obligation d'information
Axess aide le commanditaire à remplir les obligations mentionnées aux articles 32 à 36 du RGPD (sécurité du traitement, notification des violations de la protection des données personnelles à l'autorité de contrôle, notification à la personne concernée par une violation de la protection des données personnelles, analyse d'impact sur la protection des données, consultation préalable).

Sur demande, Axess met à la disposition du client toutes les informations nécessaires (par exemple certifications existantes, mesures techniques et organisationnelles, etc.) pour attester du respect des obligations mentionnées à l'article 28 du RGPD (obligations du sous-traitant). Par ailleurs, Axess permet et contribue à la réalisation d'audits, y compris des inspections, par le commanditaire ou par un autre auditeur mandaté par celui-ci.

Axess informe immédiatement le commanditaire en cas de violation du RGPD ou si Axess estime qu'une instruction du commanditaire est contraire aux dispositions de l'Union européenne ou des États membres en matière de protection des données.

5.4 Contrat de traitement des commandes
Il est assuré que les données à caractère personnel traitées pour le compte du commanditaire ne sont traitées que conformément aux instructions de ce dernier. Axess a conclu des contrats avec des parties externes pour les types de traitement des données de commande suivants :
> Traitement des données par des personnes externes
> Destruction des supports de données / élimination par des personnes externes
> Maintenance et télémaintenance par des personnes externes
> Administration / administration à distance par des personnes externes

Le traitement des données à caractère personnel pour le compte du commanditaire, uniquement selon ses instructions est garanti par les mesures suivantes.
> Instructions écrites
> Confirmation de l'offre et de la commande
> Pseudonymisation

5.5 Sous-traitant
Axess est en droit de faire appel à des sous-traitants pour le traitement des données personnelles. Toute modification envisagée concernant le sous-traitant doit être communiquée dans les temps et par écrit au commanditaire pour que celui-ci puisse s'opposer à la modification. Sont exclues de cette clause les situations dans lesquelles la notification n'est pas possible ou n'est pas réalisable (notamment en cas de danger imminent). Axess conclut un contrat écrit avec les sous-traitants et convient avec eux, mutatis mutandis, des mêmes obligations en matière de protection des données que celles présentées dans ce chapitre.
Les sous-traitants suivants sont mandatés par Axess :
https://teamaxess.com/en/security-policy-sub-processors
Dans le cas d'un contrat d'achat avec un revendeur officiel d'Axess, Axess ne fournit des données qu'au partenaire de contrat respectif (partenaire ou revendeur).

6 Fin du contrat
À la fin de la relation commerciale sous-jacente, Axess restitue au client toutes les données personnelles dans un format usuel pour le traitement des données ou les efface, à moins qu'il n'existe une obligation de conserver les données personnelles conformément au droit de l'Union européenne ou au droit d'un État membre.

7 Clauses finales
La durée du concept de sécurité est identique à celle de la relation commerciale entre Axess et le client. Ses dispositions finales s'appliquent par analogie au contrat de traitement des commandes.