MINDBAZ

Politique de sécurité

POLITIQUE DE SECURITE DES DONNEES A CARACTERE PERSONNEL DE MINDBAZ

Article 1 - Objet

MINDBAZ, société par actions simplifiée située 59 rue Nationale 59800 LILLE, enregistrée au Registre du commerce et des sociétés de LILLE MÉTROPOLE sous le numéro 893278382 et représentée par son Président Monsieur Sébastien LEMIRE ci-après « LA SOCIÉTÉ » met au centre de ses priorités et préoccupations la protection des données à caractère personnel, et a mis en place des démarches de sécurité.

Le présent document décrit la politique de sécurité mise en œuvre par LA SOCIÉTÉ relativement à l'ensemble des services qu'elle est amenée à fournir à ses clients (ci-après « les Services »).

Par conséquent, LA SOCIÉTÉ prend les précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel traitées, notamment afin d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Article 2 - Sécurité des serveurs

LA SOCIÉTÉ renforce les mesures de sécurités appliquées aux serveurs utilisés en interne ;

I.1 Habilitations

LA SOCIÉTÉ définit un ensemble de rôles (ex : administrateur, collaborateur, résident, etc.) correspondant chacun à une collection de droits d'accès, à une fonctionnalité des Services (ex : accéder aux flux de données, gérer les données patrimoniales, gérer les comptes d'accès, définir un groupe de favoris, etc.).

Il appartient au client de définir les habilitations fonctionnelles de chacun de ses utilisateurs en leur affectant tout ou partie de ces rôles.

Pour d'évidentes raisons de sécurité, les comptes d'accès sont créés par défaut avec des rôles limités. Il relève de la responsabilité des administrateurs du domaine du client d'étendre ou non les habilitations fonctionnelles de ses utilisateurs.

En interne, LA SOCIÉTÉ met en place le même système d'habilitation pour son personnel

I.2 Authentification des utilisateurs

LA SOCIÉTÉ procède à l'authentification de toute personne physique accédant à ses Services, tant ses utilisateurs clients qu'utilisateurs issus de son personnel. LA SOCIÉTÉ s'assure que toute personne physique accède uniquement aux données dont il a besoin.

LA SOCIÉTÉ fournit à chaque utilisateur des identifiant qui leurs sont propres afin de s'authentifier avant toute utilisation des moyens informatiques. Tous les accès effectués par les utilisateurs font l'objet d'une authentification préalable.

Les utilisateurs doivent produire un email identifiant ainsi qu'un mot de passe connu d'eux seuls qui est spécifié lors de la création de leur compte. LA SOCIÉTÉ permet notamment aux utilisateurs de configurer la longueur minimale des mots de passe et leur complexité afin de les rendre difficiles à deviner. Les utilisateurs peuvent également définir une durée de validité pour les mots de passe de manière à les renouveler régulièrement.

I.3 Journalisation des accès

LA SOCIÉTÉ dispose d'un dispositif de gestion des traces et des incidents qui doit être mis en place afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident.

Ainsi, LA SOCIÉTÉ enregistre, pour chaque client, certaines des actions effectuées sur les systèmes informatiques dans un journal d'accès dédié.

Ces journaux d'accès contiennent pour chaque accès (liste non exhaustive) :

● La nature de l'accès (service accédé, fonctionnalité sollicitée, paramètres transmis),

● L'identité de l'auteur de l'accès,

● Le contexte de l'accès (terminal, réseau et interface utilisés),

● Le résultat du traitement de l'accès (succès ou échec) et, le cas échéant, les motifs de l'échec (échec d'authentification, accès non habilité, paramètres erronés, service indisponible, etc.),

● La date et l'heure de l'accès.

I.4 Hébergement

L'ensemble des serveurs utilisés pour les Services mis à disposition du client et les données du Client sont hébergés par LA SOCIÉTÉ et/ou des fournisseurs de LA SOCIÉTÉ qui répondent parfaitement aux exigences du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et aux précautions édictées par la CNIL.

A la demande du client, LA SOCIÉTÉ informe précisément le client sur le lieu de localisation exacte de stockage de ses données dans le cadre des Services fournis.

I.5 Réplication des données

LA SOCIÉTÉ emploie des systèmes de stockage redondants garantissant l'existence de plusieurs copies de chaque donnée, chaque copie étant stockée sur un dispositif physique distinct des autres copies. Les données des clients sont donc toujours disponibles et accessibles même en cas d'arrêt ou de panne d'un de ces dispositifs.

I.6 Chiffrements et autres mesures techniques de sécurité

LA SOCIÉTÉ assure l'intégrité, la confidentialité et l'authenticité des données aux moyens de fonctions hachages adéquates, de signatures numériques et de méthodes de chiffrement

conformes aux recommandations de la CNIL (chiffrement fort AES ou 3DES avec une clé de 128 bits minimum).

Article 3 - Sécurité physique

LA SOCIÉTÉ prend toutes les mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications afin de renforcer la sécurité de l'intégralité des transmissions de données à caractère personnel.

A ce titre, LA SOCIÉTÉ restreint les accès aux locaux qui sont soumis à une liste d'autorisation et à un contrôle d'entrée et de sortie.

LA SOCIÉTÉ dispose également d'alarmes anti-intrusion, de détecteurs de fumées ainsi que des moyens de lutte efficace contre les incendies.

Article 4 - Sécurité des transmissions de données

LA SOCIÉTÉ maintient un niveau de sécurité élevé relativement aux transmissions de données à caractère personnel.

De manière générale, LA SOCIÉTÉ ne fait transiter aucunes données sans que le canal de communication de celles-ci ne soit sécurisé ou sans que les données ne soient chiffrées.
La transmission non chiffrée des données au travers de technologie de messagerie (messagerie instantanée, e-mail, chat, etc.) est proscrite par LA SOCIÉTÉ. Si des données sont échangées par LA SOCIÉTÉ, elles sont chiffrées à l'aide d'algorithmes de chiffrement tels que détaillés à l'article 2.6.

Lorsque LA SOCIÉTÉ échange des données au travers d'applications Web (HTTP) ou FTP, les communications sont sécurisées au moyen de TLS, mais en aucun cas à l'aide d'une version de SSL.

Les données communiquées à des sous-traitants de LA SOCIÉTÉ ou gérées par ces derniers bénéficient de garanties suffisantes au regard de la conformité au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. L'intégralité des sous-traitants de LA SOCIÉTÉ s'est engagée contractuellement envers LA SOCIÉTÉ quant aux exigences de sécurité du traitement des données.

Article 5 - Sensibilisation du personnel de LA SOCIÉTÉ

Tout le personnel de LA SOCIÉTÉ est soumis à de strictes obligations de confidentialité. Une charte interne est établie à l'attention du personnel et précise les règles et recommandations à suivre pour les respecter. Le personnel de LA SOCIÉTÉ peut faire l'objet de sanctions disciplinaires allant jusqu'au licenciement en cas de manquement aux obligations de confidentialité.

Les règles de confidentialité de LA SOCIÉTÉ précisent par ailleurs dans quelles conditions les membres du personnel de LA SOCIÉTÉ peuvent être amenés à accéder aux données des clients dans le cadre des Services. Ces accès sont restreints et font l'objet d'un contrôle rigoureux.

Article 6 - Sécurité des postes de travail

LA SOCIÉTÉ prend toutes les mesures nécessaires contre les risques d'intrusion dans les systèmes informatiques et les postes de travail qui constituent un des principaux points d'entrée.

A cet effet, LA SOCIÉTÉ dispose notamment d'un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné, d'un « pare-feu » (*« firewall »*) logiciel, d'une limitation de l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail, d'antivirus régulièrement mis à jour et d'une politique de mise à jour régulière des logiciels.

Article 7 - Sauvegarde et maintenance

LA SOCIÉTÉ sauvegarde régulièrement l'environnement de production de ses Services, ce qui inclut toutes les données des clients, sur des dispositifs d'archivage physiquement distinct des dispositifs de stockage principaux. Il est ainsi toujours possible de récupérer une version antérieure des données des clients au cas où les copies courantes seraient détruites ou altérées intentionnellement ou accidentellement.

LA SOCIÉTÉ prévoit les opérations de maintenance nécessaires pour maîtriser l'accès aux données par l'ensemble des utilisateurs.

Chaque opération de maintenance fait l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants.

En cas de télémaintenance permettant l'accès à distance aux fichiers par un tiers, LA SOCIETE est en mesure d'identifier la provenance de chaque intervention extérieure. À cette fin, le tiers opérant la maintenance s'exécute uniquement avec l'accord préalable de LA SOCIETE avant chaque opération de télémaintenance.

Des registres sont établis sous la responsabilité de LA SOCIÉTÉ, mentionnant les dates et nature détaillée des interventions de télémaintenance ainsi que les noms de leurs auteurs.

Article 8 - Continuation des Services

LA SOCIÉTÉ dispose d'un plan de continuité ou de reprise d'activité anticipant les éventuels incidents (ex : panne matérielle). Les mesures du plan sont pour l'essentiel les suivantes :

● Recrutement et formation du personnel dans une optique de redondance des compétences et des expertises clés ;

● Optimisation des plannings de façon à garantir la disponibilité permanente de chaque compétence et expertise clé ;

● Equipement du personnel à l'aide de terminaux nomades et faciles à remplacer ;

● Stockage et sauvegarde des données hors des terminaux du personnel.

Article 9 - Sécurité du réseau informatique interne

LA SOCIÉTÉ n'autorise que les services réseaux nécessaires aux différents traitements dans le cadre de ses Services. Par conséquent, LA SOCIÉTÉ a mis en place les précautions élémentaires suivantes :

- Limitation des accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.).
- Gestion des réseaux Wi-Fi avec chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boîtier générateur de mots de passe à usage unique (OTP), etc.).
- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN.
- Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.)

Article 10 - Sécurité de l'informatique mobile

LA SOCIÉTÉ prend toutes les mesures nécessaires afin d'anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.

A ce titre, LA SOCIÉTÉ sensibilise les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter.

LA SOCIÉTÉ met également en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades, pour se prémunir contre la disparition des données stockées. Enfin, LA SOCIÉTÉ prévoit des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.).

Article 11 - Sécurité des développements et des sites internet

LA SOCIÉTÉ intègre la protection des données à caractère personnel au développement informatique dès les phases de conception afin d'offrir aux personnes concernées une meilleure maîtrise de leurs données et de limiter les erreurs, pertes, modifications non autorisées, ou mauvais usages de celles-ci dans les applications.

LA SOCIÉTÉ s'assure de l'application des bonnes pratiques minimales à ses éventuels sites web et met en œuvre à ce titre le protocole TLS afin de garantir l'identité et la confidentialité des informations transmises.

LA SOCIÉTÉ limite les ports de communication strictement nécessaires au bon fonctionnement des éventuelles applications installées et limite également l'accès aux outils et interfaces d'administration aux seules personnes habilitées.

Article 12 - Violation de sécurité

Dans l'éventualité où une violation de sécurité est détectée par LA SOCIÉTÉ, celle-ci prévient immédiatement la CNIL dans les modalités de notifications prévues par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et contacte les personnes et/ou clients affectés par la situation.

LA SOCIÉTÉ met tout en œuvre pour remédier à la situation au plus vite et applique les correctifs nécessaires, dans le but de protéger les données des clients.

Article 13 - Archivage et destruction des données

LA SOCIÉTÉ archive les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux.

Aussi, LA SOCIÉTÉ définit en interne un processus de gestion des archives et met en œuvre des modalités d'accès spécifiques aux données archivées.

Si des appareils sont destinés à être mis au rebut, LA SOCIÉTÉ veille à ce que l'intégralité des données soit préalablement effacée.

Lorsque les archives sont destinées à être détruites, LA SOCIÉTÉ choisit un mode opératoire garantissant que l'intégralité d'une archive a été détruite.

Article 14 - Contact RGPD

En cas des questions relatives aux pratiques de sécurité de LA SOCIÉTÉ, vous pouvez contacter le service compétent en matière de protection des données à caractère personnel en envoyant un courrier à l'adresse suivante :

MINDBAZ
59 rue Nationale
59800 LILLE
dpo@mindbaz.com