Lawyer Cloud Act

La présente charte constitue le référentiel d'exigences applicables à tout prestataire de services informatiques ayant vocation à recueillir des données soumises au secret professionnel des avocats (les "Données") (l'"Entité").

Elle s'inspire du Guide d'hygiène informatique édicté par l'Autorité Nationale de la Sécurité des Systèmes d'Information et du Guide de la sécurité des données personnelles édicté par la Commission Nationale de l'Informatique et des Libertés.

Elle est le fruit d'une réflexion menée par la société Predictice, au terme d'une consultation de ses partenaires historiques (Incubateur du Barreau de Paris et Comité éthique et scientifique de la justice prédictive) et d'autres acteurs, tels que des membres du gouvernement et des députés disposant d'une expertise en matière numérique.

La société Predictice s'engage à faire ses meilleurs efforts pour faire respecter l'ensemble des principes édictés dans la présente charte.

Article 1. Information des équipes opérationnelles

Les équipes opérationnelles de l'Entité sont informées de la législation en vigueur, des principaux risques et menaces, du maintien en condition de sécurité, de l'authentification et du contrôle d'accès, du durcissement des systèmes, du cloisonnement réseau et de la journalisation du système.

Une charte informatique reprenant les principes édictés dans la présente charte est annexée au règlement intérieur de l'Entité.

L'Entité dispose d'un référent en sécurité des systèmes d'information, connu de tous les utilisateurs.

Article 2. Sensibilisation des utilisateurs

L'Entité informe les utilisateurs de la législation en vigueur, des principaux risques et menaces, ainsi que des règles et consignes participant à la sécurité du système.

En particulier, l'Entité sensibilise les utilisateurs aux risques liés au choix d'un mot de passe trop facile à deviner ou à la réutilisation de mots de passe d'une application à l'autre et, plus particulièrement, entre messageries personnelles et professionnelles.

Article 3. Connaissance du système d'information

L'Entité maintient à jour un schéma simplifié de l'infrastructure globale du réseau. Ce schéma permet notamment de localiser les serveurs de l'Entité stockant les Données.

L'Entité maintient également à jour un inventaire des comptes bénéficiant de droits spécifiques sur le système d'information.

Article 4. Sécurité physique du parc informatique

L'Entité met en place, sur l'ensemble de son parc informatique propre, un système d'encryptage de l'ensemble des postes. L'Entité dote ces postes d'un pare-feu local.

Les accès aux locaux de l'Entité qui contiennent son parc informatique sont contrôlés à l'aide de badges. Les accès non accompagnés des prestataires extérieurs sont proscrits. Lors du départ d'un collaborateur ou d'un changement de prestataire, il est procédé au retrait des droits d'accès ou au changement des codes d'accès.

Article 5. Sécurité des Données

5.1. Procédure d'authentification sur la plateforme de l'Entité

L'Entité met en place un système de double authentification de l'utilisateur par mot de passe et par code, récupéré par l'utilisateur sur un appareil de confiance ou après vérification de son adresse email.

Pour garantir le respect des règles de sécurité, l'Entité peut recourir à différentes mesures, parmi lesquelles le blocage des comptes à l'issue de plusieurs échecs de connexion et la désactivation des options de connexion anonyme.

5.2. Transmission chiffrée des Données

La transmission des Données recueillies par l'Entité est systématiquement chiffrée.

En outre, la transmission du secret (mot de passe, clé, etc.) permettant de déchiffrer les Données, si elle est nécessaire, est effectuée *via* un canal de confiance ou, à défaut, un canal distinct du canal de transmission des Données.

5.3. Souveraineté numérique

Les Données recueillies par l'Entité sont stockées en France, par un hébergeur ayant son siège social en France et soumis au droit français uniquement.

Article 6. Audits et exercices de sécurité

L'Entité procède régulièrement à la réalisation d'audits techniques et/ou organisationnels. L'Entité procède également chaque année à des exercices de sécurité.

A l'issue de ces audits et exercices, l'Entité applique les éventuelles actions correctives requises pour se conformer aux réglementations et obligations légales.

L'Entité applique une procédure stricte permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité. La hiérarchie et le référent en sécurité des systèmes d'information sont prévenus. Tout incident éventuel est consigné dans un registre centralisé.

Article 7. Conformité à la déontologie de la profession d'avocat

L'Entité s'engage à ce qu'un avocat, désigné par le Comité éthique et scientifique de la justice prédictive, vérifie chaque année la conformité du traitement des données opéré par l'Entité à la déontologie de la profession.

Fait à Paris, le 12 avril 2021

Pour Predictice :

Louis Larret-Chahine
Louis Larret-Chahine (13 Apr 2021 12:24 GMT+2)

Louis Larret-Chahine

Pour le Comité éthique et scientifique de la justice prédictive :

Mauricette DANCHAUD
Mauricette DANCHAUD (13 Apr 2021 11:22 GMT+2)

Mauricette Danchaud

Béatrice BRUGUES REIX
Béatrice BRUGUES REIX (14 Apr 2021 11:33 GMT+2)

Béatrice Brugués-Reix

Elisabeth Grosdhomme
Elisabeth Grosdhomme (14 Apr 2021 11:46 GMT+2)

Elisabeth Grosdhomme

Solën Guezille
Solën Guezille (13 Apr 2021 10:12 GMT+2)

Solën Guézille

Paul-Albert IWEINS
Paul-Albert IWEINS (14 Apr 2021 10:15 GMT+2)

Paul-Albert Iweins

Dominique Perben

Pimont (16 Apr 2021 13:19 GMT+2)

Sébastien Pimont

Fabrice Melleray (15 Apr 2021 10:13 GMT+2)

Fabrice Melleray