CHARTE SECURITE DE L'INFORMATION ET PROTECTION DES DONNEES PERSONNELLES APPLICABLE AUX FOURNISSEURS

Préambule

L'objectif de cette charte est de rappeler les engagements et exigences minimaux en matière de confidentialité, sécurité de l'information et de protection des données à caractère personnel qui s'appliquent aux fournisseurs, partenaires et prestataires désignés ci-après par « Le fournisseur », dans les cas suivants :

- Accès de manière directe ou indirecte à de l'information Luminess ou des clients de Luminess,
- Participation au bon fonctionnement du système d'information Luminess,
- Fourniture de services en mode SAAS pour Luminess ou ses clients, ou indispensables au maintien des services rendus aux clients de Luminess
- Accès aux locaux Luminess.

Documents de référence

- Politique de sécurité des systèmes d'information
- Charte utilisateur et charte administrateur
- Modèle de NDA
- Modèle d'engagement individuel de confidentialité
- Procédure d'accès aux locaux Luminess.

Cadre général

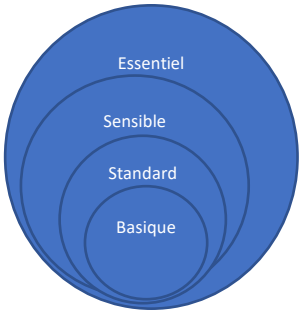
Le fournisseur s'engage à respecter les politiques Jouve en termes de sécurité de l'information et de protection des données à caractère personnel. Cela inclut de manière implicite la confidentialité et le respect de la propriété industrielle.

En cas d'accès ou de traitement de données à caractère personnel, et ce quel qu'en soit le support, la Loi Informatique & Liberté et le règlement général sur la protection des données (RGPD) s'appliquent.

Qualification des fournisseurs

Les fournisseurs sont qualifiés de la manière suivante :

- Basique
- Standard
- Sensible
- Essentiel



Fournisseur standard

Le fournisseur qualifié de standard s'engage à :

- Signer un engagement de confidentialité et de non-exploitation avec la personne morale (NDA) dans le cas d'accès au SI Luminess ou aux locaux
- Communiquer sur tout incident de sécurité pouvant impacter directement ou indirectement les informations ou les activités de Luminess
- Communiquer sur les changements apportés impactant le service ou le niveau de sécurité
- Respecter les engagements de service si applicable avec pénalités
- Disposer d'une assurance en RC « appropriée au regard des prestations »
- Garantir le respect des règles de sécurité dans le cas d'accès au SI Luminess ou aux locaux avec fixation d'indemnités forfaitaires
- Suivre le processus de réversibilité si applicable
- Respecter les règles et procédures d'habilitation et d'accès au système d'information et aux locaux
- Reporter toutes les causes précitées sur tous les sous-traitants éventuels du fournisseur.

Fournisseur sensible

Le fournisseur qualifié de sensible s'engage de plus à :

- Faire signer un engagement de confidentialité individuel (NDA renforcé) à chaque collaborateur pouvant accéder à des données Luminess ou client ou aux locaux Luminess

- Accepter de se faire auditer par Luminess, un client, une autorité administrative ou un cabinet d'audit mandaté dans la limite d'1 fois /an
- Pour les fournisseurs accédant au système d'information ou à des données Luminess prendre connaissance de la charte informatique et faire signer la charte administrateur à chacun des intervenants
- Fournir un Plan d'Assurance Sécurité si des exigences spécifiques sont identifiées
- Être conforme à l'ISO 27001 pour les fournisseurs dont le domaine d'activité est l'IT
- Disposer d'une assurance en RC solide souscrite auprès d'une compagnie d'assurance internationale réputée
- Pour les fournisseurs de solutions en SaaS, en cas d'hébergement de données personnelles ou sensibles, lieu d'hébergement des données situé en UE
- Disposer d'un RSSI et d'un DPO en cas de traitement de données à caractère personnel.

Fournisseur essentiel

Le fournisseur qualifié d'essentiel s'engage de plus à :

- Fournir un Plan d'Assurance Sécurité
- Être certifié ISO 27001 (et maintenir sa certification) ou engagé dans le processus
- Pour les fournisseurs dont le domaine d'activité est l'IT, disposer d'une assurance Cyber solide souscrite auprès d'une compagnie d'assurance internationale réputée et fournir les certificats correspondants à la demande de Luminess
- Pour les fournisseurs de solutions en SaaS, en cas d'hébergement de données personnelles ou sensibles, héberger les données en France et les chiffrer
- Disposer d'un Plan de Continuité d'Activité (PCA) sur le périmètre de la prestation. Ce PCA est communicable à Luminess sur demande.

Audit et contrôle

Le Fournisseur accepte que LUMINESS le contrôle ou l'audite sur le périmètre de la prestation.

En cas de non-conformité, le Fournisseur propose un plan de remédiation à Luminess sous 10 jours ouvrés.