Version : 1.0 du 28 octobre 2016

TERMES RELATIFS AU TRAITEMENT DE DONNÉES DANS LE CADRE DE LA SOLUTION INTERNE

1. Introduction :

Par les présentes dispositions, Gemalto désire renseigner le client sur le traitement des données, qui comprennent des données personnelles (définies ci-dessous), auxquelles Gemalto peut accéder dans le cadre de la prestation du service de support (défini ci-dessous) relatif à la solution interne (définie ci-dessous) qu'il fournit au client.

2. Définitions

Les termes suivants sont utilisés à la présente.

Composant d'arrière-plan : tout composant qui s'exécute dans les locaux du client où la solution interne est installée est considéré comme un composant d'arrière-plan aux fins de la présente. Les composants d'arrière-plan comprennent les serveurs d'application, les serveurs de base de données, les composants de l'infrastructure sous-jacente, tels que les routeurs, les coupe-feux ainsi que les coupe-feux des applications Web s'ils font partie de la prestation du service de Gemalto au client.

Renseignements du client : renseignements personnels que Gemalto peut recueillir lors de ses interactions avec les employés ou les agents du client dans le cadre des services de support.

Lois sur la protection des données personnelles : ensemble des lois, des règles, des règlements, des exigences gouvernementales, des codes, des lois des États ainsi que des lois internationales, fédérales et provinciales qui visent les données personnelles.

Solution interne : solution de Gemalto pour laquelle le client a obtenu une licence et qui est installée dans les locaux du client et gérée par le client.

Système de gestion : système de gestion des incidents sur plate-forme Web, appelé STiM, que Gemalto utilise pour la prestation des services de support.

Données personnelles : ce terme désigne (i) les données relatives à une personne vivante (liées à sa vie personnelle ou familiale, à son entreprise ou à sa profession) pouvant être identifiée (a) à partir de ces données, ou (b) à partir de ces données et d'autres renseignements dont le contrôleur de données dispose, ou dont il pourrait éventuellement disposer, ainsi que (ii) les renseignements pouvant être utilisés pour identifier ou retracer l'identité d'une personne, y compris, mais sans s'y limiter, son nom, son adresse, son numéro d'assurance sociale, ses données biométriques, sa date de naissance, etc.

Support à distance : utilisation du téléphone, du courrier électronique ou d'un RPV (réseau privé virtuel) pour faciliter la résolution d'une demande.

Demande : requête transmise par le client afin de se prévaloir du service de support.

Dossier de la demande : dossier du système de gestion, généré par Gemalto pour consigner une demande et en faire le suivi.

Données du service : données conservées dans la solution interne, auxquelles Gemalto a accès pour assurer les services de support.

Centre de services : groupe de support technique de Gemalto, qui constitue le point de contact unique entre Gemalto et le client pour la gestion de la totalité des demandes du client, des communications avec le client et des remontées hiérarchiques auprès du client.

Service de support : service de support déterminé par l'accord sur les niveaux de service.

RPV : réseau privé virtuel offrant un mécanisme de communications sûr pour la transmission de données et d'autres renseignements entre deux points d'extrémité.

3- **Traitement des renseignements du client**

Lorsqu'une demande est transmise, Gemalto recueille les Renseignements du client qui sont enregistrés dans le système de gestion situé en France. Le but de cette collecte de données est de déterminer l'origine de la Demande et d'associer la Demande au client dans le but d'analyser, de diagnostiquer et de résoudre la Demande, de facturer le client ainsi que d'améliorer la solution interne et la sécurité.

Les renseignements du client peuvent être transférés à l'équipe de support qui assure le service de support, ce qui déclenchera un transfert transfrontalier de données, conformément aux clauses de la section 6 ci-dessous.

4- **Support à distance**

Le service de support est assuré par un centre de services (support de niveau 1) situé en Inde chez SAFENET INFOTECH PVT LTD (entité juridique faisant partie du groupe de sociétés de Gemalto). Le centre de services crée un dossier de demande dans le système de gestion, puis coordonne la réponse en fonction de l'accord sur les niveaux de service ayant été conclu.

La demande peut faire l'objet d'une remontée hiérarchique au support de niveau 2 ; les experts responsables du support de niveau 2 se trouvent dans les localisations précisées par Gemalto au cas par cas, dans le contrat ou la proposition commerciale le cas échéant.

Si Gemalto estime que la demande nécessite une connexion à distance à la solution interne, Gemalto accédera à la solution interne à l'aide d'un RPV sécurisé déjà installé chez le client.

Pour qu'il soit possible de traiter la demande, le client doit donner à Gemalto l'accès à la solution interne au besoin.

La connexion à distance permettant d'accéder à la solution interne est visée par les clauses relatives à la sécurité, décrites à la section 5 ci-dessous.

Si le client s'attend à ce que Gemalto respecte une politique sur la sécurité ou un processus de support qu'il a établi, s'il y a lieu, alors Gemalto se réserve le droit de vérifier la politique ou le processus, puis :

a) confirmera qu'il peut s'y conformer (moyennant des frais additionnels) ; ou

b) s'il est incapable de s'y conformer, Gemalto ne sera pas tenu de respecter la politique ou le processus.

Lors de l'utilisation d'une connexion à distance pour accéder à la solution interne, Gemalto peut voir et utiliser les données du service uniquement afin d'assurer le service de support. Gemalto ne copiera pas les données du service, ne les modifiera pas et ne les supprimera pas.

5- **Clauses relatives à la sécurité**

5.1 Le service de support est fondé sur les principes de sécurité suivants :

- seules les personnes ayant besoin d'un accès à distance sont autorisées à l'utiliser ;
- seules les actions autorisées peuvent être effectuées ;
- l'accès à la solution interne se fait au moyen d'une interface fiable ;
- les activités suspectes sont surveillées ;
- les actions font l'objet d'un suivi afin d'établir les rôles et les responsabilités lors d'une enquête.

Plus précisément :

5.1.1 Cloisonnement

Dans le but d'isoler la solution interne de l'infrastructure de Gemalto, Gemalto propose deux solutions :

a) La première utilise un serveur administratif sécurisé, qui bloque les accès directs entre la solution interne et les PC des opérateurs. Les opérations peuvent s'effectuer uniquement à partir du serveur administratif sécurisé. Puisque l'opérateur n'a aucun droit administratif pour le serveur administratif sécurisé, il peut utiliser uniquement le logiciel autorisé déjà installé sur ce serveur.

b) La deuxième solution utilise une infrastructure dédiée. L'opérateur travaille sur un PC dédié, pour lequel il détient des droits limités. Des logiciels spécifiques sont préinstallés sur ce PC pour l'exécution des opérations de maintenance et de support. Un serveur de fichiers permet de transférer les fichiers journaux. Un logiciel antivirus est aussi installé sur le PC dédié afin d'éviter que le PC soit infecté.

Ces deux solutions visent à limiter autant que possible l'utilisation d'applications inappropriées et le transfert de fichiers ne devant pas être transférés entre la solution interne et les locaux de Gemalto.

Le second aspect de ce cloisonnement porte sur le support entre les infrastructures. La voie de communication doit aussi être protégée. L'utilisation d'un RPV est obligatoire pour les deux solutions afin de protéger le lien entre la solution interne et les locaux de Gemalto.

5.1.2 Authentification

Un autre aspect important est l'authentification de l'opérateur. Cette authentification doit être assez robuste, afin d'éviter toute usurpation d'identité, et exécutoire en cas de procédures judiciaires.

Gemalto a mis en place son propre système basé sur sa méthode d'authentification à deux facteurs de forme. La passe personnelle de l'employé lui donne accès au PC dédié ou au serveur administratif sécurisé. Cette passe unique contient une clé privée intégrée servant à l'authentification.

Pour avoir accès aux systèmes, l'opérateur doit présenter sa passe et composer le NIP associé. Combinée à un LDAP (protocole allégé d'accès annuaire) central, la passe offre plusieurs avantages. Le premier consiste en la validation de la passe. Le deuxième avantage est de permettre la gestion de groupes. En fonction de l'authentification LDAP, le système valide les droits de l'opérateur quant à l'accès au serveur administratif sécurisé et à la solution interne. Un troisième avantage est de faciliter la gestion des accès. Les accès des nouveaux employés et la gestion de la révocation des autorisations s'effectuent dans le système central. Grâce à cette méthode d'authentification robuste, Gemalto garantit que seules les personnes autorisées accèdent à la solution interne. De plus, en fonction des définitions des rôles et des groupes, les droits d'accès sont limités à la prestation du service de support.

5.1.3 Vérifiabilité

À cette authentification robuste s'ajoute la possibilité de détecter en temps réel les comportements suspects ou d'effectuer des analyses supplémentaires lors d'un incident.

La détection en temps réel est basée sur des détecteurs de sécurité, qui envoient des alertes de sécurité. Ces alertes déclenchent un processus interne pour déterminer la criticité de la détection et lancer les actions de confinement adéquates.

Les systèmes de journalisation consignent les actions effectuées par les opérateurs. Grâce au système d'authentification robuste, les journaux associent chaque action à la personne qui l'a effectuée.

En raison de la confidentialité de certaines données, les journaux sont filtrés. Ces journaux sont conservés dans un espace sécurisé ; seuls les responsables de la sécurité y ont accès.

Ces systèmes combinés permettent à Gemalto de détecter les alertes de sécurité et d'y réagir.

5.2 Attestation du client

Le client reconnaît et comprend que tous les composants d'arrière-plan de la solution interne offerte par Gemalto doivent s'exécuter dans un environnement sécurisé et contrôlé. Cet environnement doit être conçu conformément aux meilleures pratiques relatives à chacun de ses aspects, de la sécurité physique à la sécurité logique. Gemalto a adopté la norme ISO 27002 quant aux meilleures pratiques en matière de sécurité. La solution interne comprend des caractéristiques de sécurité spécifiques que Gemalto peut fournir sur demande. Le client accepte d'assumer toutes les responsabilités s'il ne met pas en place les caractéristiques de sécurité susmentionnées ou s'il omet de demander les caractéristiques de sécurité spécifiques de la solution interne.

6- **Transfert transfrontalier**

6.1 Comme indiqué à la section 4 ci-dessus, la prestation du service de support peut entraîner un transfert transfrontalier des renseignements du client et/ou des données de support. Le client comprend qu'un tel transfert transfrontalier des renseignements du client et/ou des données de support peut être visé par des exigences particulières imposées par les lois sur la protection des données personnelles et qu'il incombe au client de se conformer à ces exigences à titre d'entité qui fournit les renseignements du client et/ou les données de support à Gemalto.

6.2 Dans l'éventualité d'un transfert transfrontalier des renseignements du client et/ou des données du service, il pourrait être obligatoire de conclure un accord de transfert transfrontalier spécifique en vertu des lois applicables sur la protection des données personnelles. Gemalto et le client collaboreront afin de respecter cette exigence.
