Version : 1.0 du 28 octobre 2016

Termes relatifs au traitement de données dans le cadre des services gérés[1]

Le client (défini ci-dessous) accepte les présentes clauses de traitement de données, y compris les annexes jointes (collectivement, les « CTD »), parce qu'il a conclu un accord de service (défini ci-dessous) avec la société (définie ci-dessous). Le client et la société s'engagent à respecter ces CTD à compter de la date d'entrée en vigueur de l'accord de service. Si l'accord de service a été conclu avant la date d'entrée en vigueur définie ci-dessus et que la durée de l'accord de service doit être prolongée, alors ces CTD remplaceront toute clause de traitement de données signée antérieurement par le client et la société.

Ces CTD sont toujours intégrées à un accord de service à titre de référence. En cas de conflit ou de divergence entre les clauses de l'accord de service et les CTD, alors les CTD auront toujours préséance. Nous recommandons au client de lire les CTD. Si le client est en désaccord avec certaines clauses, il est invité à transmettre ses remarques et ses commentaires avant la signature de l'accord de service. Si la société et le client acceptent de modifier les CTD, la modification ayant été convenue sera jointe en annexe à l'accord de service.

1- Raison d'être des CTD

La solution (définie ci-dessous), qui consiste en des logiciels ou en une combinaison de logiciels et de matériel, permet d'effectuer le traitement des données personnelles du client (définies ci-dessous) de façon que la solution profite au client et, dans le cas d'une offre du client (définie ci-dessous) aux utilisateurs finaux (définis ci-dessous).

La solution peut être hébergée par une entité d'hébergement (définie ci-dessous) non contrôlée par la société. La section 4 ci-dessous explique en détail le rôle de l'entité d'hébergement.

Le client et la société reconnaissent et acceptent que les lois sur protection des données personnelles (définies ci-dessous) puissent s'appliquer au traitement des données personnelles du client. Dans un tel cas, les CTD sont applicables.

2- Définitions

Nonobstant toute définition contraire figurant dans l'accord de service, les termes définis ci-dessous et utilisés dans les présentes CTD, qu'ils soient au singulier ou au pluriel, auront les significations suivantes dans le contexte des présentes CTD :

Lois applicables sur la protection des données : lois sur protection des données personnelles qui visent le client ainsi que le contrôleur de données responsable des données personnelles.

Employés autorisés : employés du groupe Gemalto ayant besoin d'en connaître ou ayant un accès quelconque aux données personnelles du client afin d'exécuter l'accord de service.

Personnes autorisées : ce terme désigne (i) les employés autorisés, et (ii) tout sous-traitant ultérieur ayant besoin d'en connaître ou ayant un accès quelconque aux données personnelles du client afin d'exécuter l'accord de service.

Infraction à la sécurité : acquisition non autorisée ou utilisation non autorisée (i) de données non cryptées ou (ii) de données électroniques cryptées, ainsi que de la clé ou du processus confidentiel, pouvant compromettre la sécurité, la confidentialité ou l'intégrité des renseignements personnels, par une personne qui crée un risque considérable de vol d'identité ou de fraude contre une autre personne.

[1] Modèle de prestation des services gérés : la prestation des services s'effectue à l'extérieur des locaux du client.

Renseignements du client : renseignements personnels pouvant être obtenus lors des interactions entre les employés ou agents du client et le groupe Gemalto pour la prestation des services de support et de maintenance.

Société : entité juridique qui est membre du groupe Gemalto et qui a conclu l'accord de service.

Client : entité juridique qui a conclu l'accord de service.

Données personnelles du client : données personnelles contenues dans les données directement transmises à la solution par le client, ou en son nom, ou par les utilisateurs finaux.

Offre du client : services offerts aux utilisateurs finaux par le client.

Centre de données : locaux appartenant au groupe Gemalto dans lesquels la solution est installée.

Contrôleur de données : personne physique ou morale qui détermine à quoi serviront les données personnelles et la façon de les traiter.

lois sur 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.

Contrat type de l'UE : clauses contractuelles types (sous-traitants) pour le transfert des données personnelles aux sous-traitants établis dans des pays tiers qui n'offrent pas un degré de protection adéquat.

Utilisateurs finaux : personnes physiques ou morales qui acceptent l'offre du client.

RGPD : règlement général sur la protection des données (2016/679) du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Groupe Gemalto : une ou plusieurs entités juridiques individuelles ou collectives contrôlées par Gemalto N.V., une société régie par les lois des Pays-Bas. Dans ce contexte, le contrôle désigne la propriété directe ou indirecte (grâce à un ou plusieurs tiers successifs) de : (a) plus de cinquante pour cent (50 %) des actions en circulation avec droit de vote pour l'élection des directeurs ou de toute autre autorité de gestion de l'entité visée ; ou (b) dans le cas d'une entité n'ayant pas d'actions en circulation (par ex., partenariat, entreprise commune ou association non constituée en personne morale), plus de cinquante pour cent (50 %) de la part des capitaux propres permettant de prendre des décisions pour l'entité visée.

Entité d'hébergement : entité juridique non signataire de l'accord de service, qui a conclu un accord de sous-traitance avec l'administrateur de système afin d'héberger la solution.

Procédure judiciaire : demande de divulgation des données, effectuée en vertu d'une loi, d'un règlement gouvernemental, de l'ordonnance d'un tribunal, d'une citation à comparaître, d'un mandat, d'une demande transmise par un organisme de réglementation gouvernemental ou d'un organisme public, ou d'une autorité juridique, d'une procédure judiciaire ou d'un processus valable similaire.

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. Cette définition peut être modifiée en fonction des lois applicables sur la protection des données personnelles (par exemple, certaines lois sur la confidentialité des données s'appliquent non seulement aux individus, mais aussi aux entités juridiques, et non seulement aux personnes vivantes, mais aussi aux personnes décédées).

Programme de sécurité : programme de sécurité défini à l'**annexe 1** des présentes CTD.

Accord de service : accord conclu entre le client et la société.

Données du service : données conservées dans la solution et auxquelles Gemalto a accès afin de fournir les services de support et de maintenance (y compris les environnements cloud ainsi que les environnements de test, de développement et de production pouvant être accédés pour fournir les services de support et de maintenance convenus).

Solution : système d'information servant à conserver, gérer, utiliser et recueillir les données personnelles du client et les données du service.

Sous-traitant ultérieur : entité juridique engagée dans le but de fournir des services spécifiques pouvant nécessiter le traitement des données personnelles du client.

Administrateur de système : entité juridique membre du groupe Gemalto, qui est responsable de la maintenance, de la configuration et de la fiabilité de fonctionnement de la solution, comme l'installation, la mise à niveau des composants informatiques et des logiciels, l'automatisation et le respect des politiques de sécurité.

Services spécifiques : certains services décrits dans l'accord de service, autres que les tâches de l'administrateur de système, tels que (a) la prestation du service de support technique pour résoudre des problèmes spécifiques ayant été signalés, et (b) la transmission d'un rapport global statistique et analytique.

Réclamation de tiers : demande ou revendication d'un tiers qui réclame, de plein droit, un paiement en espèces ou autre.

3- **Contrôleur de données et sous-traitant responsable du traitement des données**

3.1 Le client est le contrôleur de données en ce qui concerne les données personnelles du client. La société, par l'intermédiaire des sous-traitants ultérieurs qu'elle a engagés, est le sous-traitant responsable du traitement des données personnelles du client. De plus, l'administrateur de système, par l'intermédiaire de l'entité d'hébergement qui a été engagée ou du centre de données, pourrait effectuer le traitement des données personnelles du client, à tout le moins en permettant au client de conserver les données personnelles du client dans la solution.

3.2 Dans certains cas, le client sera connecté directement à la solution et assurera alors directement, ou permettra aux utilisateurs finaux d'assurer, la prestation de la solution au moyen des données personnelles du client.

3.3 Ni la société, ni les sous-traitants ultérieurs, ni l'administrateur de système et ni l'entreprise d'hébergement ne recueillent les données personnelles du client. Les sous-traitants ultérieurs et l'administrateur de système traitent les données personnelles du client à titre de sous-traitants responsables du traitement des données sur les instructions du client et avec l'autorisation préalable du client, conformément aux clauses de l'accord de service.

4- **Exigences en matière de transparence**

4.1 Avant de conclure l'accord de service avec le client, la société remettra au client un document intitulé « Formulaire de traitement de données » ; un exemple est joint à l'**annexe 2** des CTD. Ce document décrit le type de données personnelles du client à traiter au moyen de la solution, le nom et l'emplacement de l'entité d'hébergement ou du centre de données où la solution est hébergée, les noms de l'administrateur de système et des sous-traitants ultérieurs qui traiteront les données personnelles du client, la façon dont les données personnelles du client seront traitées, les flux de données contenant les données personnelles du

client et la période de temps pendant laquelle les données personnelles du client sont conservées pendant la durée de l'accord de service ainsi qu'après l'expiration ou la résiliation de l'accord de service.

4.2 Quand le formulaire de traitement de données est approuvé, il est annexé à l'accord de service, dont il fait partie intégrante.

5- **Instructions du client**

5.1 Les données personnelles du client doivent être traitées conformément aux instructions du client. L'accord de service décrit les instructions du client quant au type, à l'étendue et à la méthode de traitement des données personnelles du client, en tenant compte des spécifications de la solution faisant l'objet de l'accord de service et du contenu du formulaire de traitement de données (décrit à la section 4 ci-dessus). Sauf disposition contraire aux présentes CTD, ni la société, ni les sous-traitants ultérieurs, ni l'administrateur de système et ni l'entreprise d'hébergement ne vérifieront, partageront ou distribueront les données personnelles du client et n'y feront pas référence.

5.2 Tout changement apporté au traitement des données personnelles pendant la durée de l'accord de service doit être préalablement approuvé par écrit par le client.

6- **Entité d'hébergement et centre de données**

6.1 En ce qui a trait aux données visées par les CTD, le formulaire de traitement de données (décrit à la section 4 ci-dessus) indique chaque entité d'hébergement qui a conclu, directement ou indirectement, un accord d'hébergement spécifique avec chaque administrateur de système concerné.

6.2 Le client utilise la solution hébergée dans le système de l'entité d'hébergement ou du centre de données pour transmettre ou traiter les données personnelles du client. Il faut noter que l'entité d'hébergement et le centre de données ne déterminent pas et ne connaissent pas les types de données conservées par le client et/ou la façon dont les données sont accédées, échangées, traitées ou classées.

7- **Sous-traitants ultérieurs**

7.1 En fonction des services spécifiques fournis au client, la société peut engager des sous-traitants ultérieurs pour fournir, en tout ou en partie, les services spécifiques.

7.2 En ce qui concerne les services de support technique faisant partie des services spécifiques, le client doit tenir compte des clauses figurant à l'**annexe 3**, qui décrivent les pratiques de l'organisation mondiale responsable du support (« OMRS ») du groupe Gemalto quant aux services de support et de maintenance.

7.3 Si des statistiques associées à un rapport global et/ou des services spécifiques de production de rapports aux fins de facturation sont offerts dans le cadre des services spécifiques, la prestation de ces services spécifiques nécessitera l'utilisation d'un logiciel qui permettra (i) d'accéder aux bases de données de production de la solution de façon sûre et (ii) d'extraire certaines données qui seront conservées dans un entrepôt de données situé dans les locaux du groupe Gemalto, où les données seront analysées pour créer les tableaux de bord et rapports convenus, en format sommaire. Si ces statistiques et services de rapports sont offerts dans le cadre de l'accord de service, ils seront indiqués sur le formulaire de traitement de données, décrit à la section 4 ci-dessus ; l'emplacement de l'entrepôt de données et l'identité du sous-traitant ultérieur seront aussi indiqués.

7.4 L'intervention d'un sous-traitant ultérieur nécessite l'autorisation écrite préalable du client, qui sera donnée avec sa signature de l'accord de service.

7.5 Si le sous-traitant ultérieur est établi dans un pays non adéquat (pays réputé ne pas offrir un degré de protection adéquat pour les données personnelles, selon la définition de la directive 95/46/CE de l'Union européenne ou du RGPD), alors la société veillera à ce que le sous-traitant ultérieur conclue un accord directement avec le client selon le contrat type de l'UE. Veuillez noter que la présente section s'appuie sur le droit européen quant à la confidentialité des données. Ces directives peuvent donc ne pas s'appliquer dans certains territoires.

7.6 Si la société et le client ont déjà conclu un accord de service et que la société envisage d'engager un nouveau sous-traitant ultérieur, alors la société en informera le client en lui fournissant des renseignements détaillés sur ce sous-traitant ultérieur et sur la partie de l'accord de service qui sera sous-traitée, et demandera l'approbation écrite du client au moyen d'une modification à l'accord de service. Si le client s'oppose à l'engagement du nouveau sous-traitant ultérieur, il devra en informer immédiatement la société par écrit. Immédiatement après avoir été informée de l'opposition du client, la société devra collaborer avec le client pour trouver une solution de rechange.

8- **Transmission des données personnelles à d'autres pays**

8.1 Comme indiqué à la section 4 ci-dessus, la solution est hébergée par une entité d'hébergement ou par un centre de données. L'utilisation de la solution par le client peut entraîner un transfert transfrontalier des données personnelles du client. Le client comprend qu'un tel transfert transfrontalier des données personnelles du client peut être visé par des exigences particulières imposées par les lois applicables sur la protection des données personnelles et qu'il incombe au contrôleur de données de se conformer à ces exigences.

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

9- **Engagements du client**

9.1 Le client déclare et certifie que les données personnelles du client qu'il fournit aux fins du traitement peuvent être traitées licitement (par ex., collecte licite, respect de l'obligation d'informer et respect des lois applicables sur la protection des données personnelles).

9.2 Le client doit s'assurer que, en raison de ses actions ou de ses inactions, la société, l'administrateur de système, le sous-traitant ultérieur, l'entité d'hébergement et le centre de données ne commettent aucune violation des lois sur protection des données personnelles en ce qui a trait au traitement des données personnelles du client.

10- **Principes de sécurité**

10.1 Conformément au programme de sécurité et dans la limite de ce programme, le groupe Gemalto met en place des mesures techniques et organisationnelles afin de protéger les données personnelles du client contre toute infraction à la sécurité. Le client convient qu'il est entièrement responsable de la façon dont il utilise la solution pour le traitement des données personnelles du client, y compris les informations d'authentification de son compte, et que la société, l'administrateur de système, le sous-traitant ultérieur, l'entité d'hébergement et le centre de données n'ont aucunement l'obligation de protéger les données personnelles du client que le client conserve ou transfère ailleurs que chez le sous-traitant ultérieur, l'entité d'hébergement et le centre de données.

10.2 La société prendra les mesures appropriées pour assurer que l'administrateur de système, le sous-traitant ultérieur, l'entité d'hébergement et le centre de données se conforment au programme de sécurité, dans la mesure où le programme s'applique à l'exécution de leurs tâches.

10.3 (a) Si la société prend connaissance d'une infraction à la sécurité, elle en avisera promptement le client et prendra des mesures raisonnables pour réduire au minimum les dommages et pour assurer la sécurité des données personnelles du client. Toute notification d'infraction à la sécurité sera transmise soit aux coordonnées indiquées à cet effet par le client dans l'accord de service ou, à la discrétion de la société, en communiquant directement avec le client (par ex., appel téléphonique ou rencontre en personne). Le client reconnaît qu'il lui incombe entièrement de s'assurer que les coordonnées mentionnées ci-dessus sont à jour et valables et de respecter ses obligations de notification à des tiers. L'obligation de la société de signaler une infraction à la sécurité ou d'y réagir en vertu de la présente section 10.3 ne doit pas être interprétée comme constituant, de la part de la société, une admission de faute ou de responsabilité quant à l'infraction à la sécurité.

(b) Dès que possible après l'envoi de la notification de la société au client quant à l'infraction à la sécurité, le client et la société devront coordonner leurs efforts afin d'enquêter sur l'infraction à la sécurité. La société mènera l'enquête et acceptera de collaborer de façon raisonnable avec le client quant au traitement de l'infraction à la sécurité, y compris, mais non de façon limitative : (i) apporter son assistance lors d'une enquête ; (ii) fournir au client un accès physique aux installations et aux opérations touchées qui sont contrôlées par le groupe Gemalto ; (iii) organiser des interviews avec les personnes autorisées ; et (iv) donner accès aux dossiers, journaux, fichiers, rapports de données et autres matériels pertinents qui concernent le client et qui sont requis afin de respecter les lois et règlements applicables sur la protection des données personnelles ou que le client pourrait raisonnablement exiger.

10.4 Nonobstant toute disposition contraire dans l'accord de service ou le programme de sécurité, les obligations de la société, du sous-traitant ultérieur, de l'administrateur de système, de l'entité d'hébergement et du centre de données portent uniquement sur les systèmes, réseaux, périphériques du réseau, installations et composants sur lesquels ils exercent un contrôle. Le programme de sécurité ne s'applique pas aux éléments suivants : (i) les données personnelles du client qui sont transmises à la société, au sous-traitant ultérieur, à l'administrateur de système, à l'entité d'hébergement et au centre de données, mais qui ne sont pas conservées dans la solution ; (ii) les données personnelles du client sur le réseau privé virtuel (RPV) du client ou sur un réseau tiers, ou (iii) les données personnelles du client traitées par le client ou ses utilisateurs, si ce traitement contrevient à l'accord de service ou au programme de sécurité.

10.5 Si le client désire procéder à une vérification du programme de sécurité, il devra envoyer sa demande à la société aux coordonnées indiquées dans l'accord de service. Plus particulièrement, la société (par l'intermédiaire de son service de sécurité d'entreprise) et le client discuteront et conviendront à l'avance de l'identité d'un vérificateur tiers indépendant et qualifié qui effectuera la vérification, d'une date de début raisonnable (c.-à-d. au moins trente [30] jours calendaires à compter de la date de réception par la société de la demande de vérification), de la portée et de la durée de la vérification ainsi que des procédures de sécurité et de confidentialité applicables à la vérification. Le client est informé que la vérification du programme de sécurité tiendra compte des règles et politiques de sécurité de chaque entité d'hébergement, du centre de données et de chaque sous-traitant ultérieur, qui peuvent limiter la portée prévue de la vérification du client. La société (par l'intermédiaire de son service de sécurité d'entreprise) peut fournir des détails sur ces limites, le cas échéant. La société ne sera pas responsable des coûts assumés par le client ni des frais facturés par un vérificateur tiers engagé par le client pour la vérification. Au cours d'une (1) année civile, la première demande de vérification d'un client est gratuite, mais la société se réserve le droit de facturer des frais et des coûts pour les demandes de vérification subséquentes.

10.6 Les données personnelles du client sont visées par des obligations de confidentialité en vertu du programme de sécurité. Par conséquent, toute infraction à la sécurité portant atteinte aux données personnelles du client ne sera pas soumise à la clause de confidentialité de l'accord de service qui porte sur les données et les renseignements considérés comme des renseignements confidentiels. La présente section 10.6 aura préséance en cas de conflit avec la clause de confidentialité de l'accord de service.

11- **Collaboration pour les requêtes et les demandes**

11.1 La société informera le client promptement (et, en tout cas, au plus tard cinq (5) jours calendaires après la réception d'une plainte, d'une requête ou d'une demande) de toute plainte, requête ou demande transmise par des individus, y compris, mais sans s'y limiter, les demandes de correction, de suppression ou de blocage de données personnelles du client. La société ne répond pas directement aux individus, sauf si le client lui a donné des instructions en ce sens, à moins que la société, le sous-traitant ultérieur, le centre de données, l'entité d'hébergement ou l'administrateur de système soit tenu de répondre en vertu de la loi ou d'une procédure judiciaire ; dans ce cas, la réponse sera transmise en respectant un laps de temps raisonnable conformément aux lois applicables. La société collaborera avec le client pour traiter et résoudre les plaintes, les requêtes et les demandes.

12- **Confidentialité, archivage et destruction des données personnelles**

12.1 La société, le sous-traitant ultérieur, le centre de données, l'entité d'hébergement et l'administrateur de système ne divulgueront pas les données personnelles du client à un tiers de quelque façon que ce soit sans l'autorisation écrite préalable du client, sauf si (i) cette divulgation est nécessaire pour l'exécution de l'accord de service, ou si (ii) conformément à la section 10 ci-dessus, il faut divulguer les données personnelles du client à une autorité publique compétente en vertu d'une procédure judiciaire.

12.2 En principe, la société, le sous-traitant ultérieur, le centre de données, l'entité d'hébergement et l'administrateur de système, conformément aux exigences des lois applicables, ne conservent pas les données personnelles du client plus longtemps que nécessaire aux fins pour lesquelles le client avait confié ses données personnelles à la société, conformément à l'accord de service ou, selon le cas, dans les limites des normes PCI-DSS et PCI-CP ou des exigences de VISA et MASTERCARD ou de tout autre exploitant de réseau de cartes de paiement.

12.3 Après les délais décrits à la section 12.2 ci-dessus, les données personnelles seront détruites définitivement.

12.4 Si le client demande que les données personnelles du client soient archivées, la société et le client devront conclure un accord d'archivage comprenant, mais sans s'y limiter, les clauses suivantes :

a) la durée d'archivage ;
b) le type d'unité de stockage ;
c) l'emplacement ;
d) les conditions d'accès ;
e) les conditions tarifaires.

13- **Traitement des coordonnées d'affaires**

13.1 Le client reconnaît et accepte que ses employés et ses agents puissent avoir des contacts avec la société et les sous-traitants ultérieurs et que, ce faisant, ils pourraient divulguer les renseignements du client. Les renseignements du client serviront à exécuter l'accord de service, à superviser et à administrer les achats ainsi qu'à administrer les services visés par l'accord de service.

13.2 Conformément à la section 13.1 ci-dessus, le client déclare et certifie par la présente qu'il a obtenu tous les consentements nécessaires aux fins énoncées à la section 13.1 ci-dessus, et qu'il autorise expressément l'utilisation des données personnelles à ces fins ainsi que la cession et le transfert des renseignements du client, à l'intérieur d'un pays ainsi que d'un pays à un autre, selon ce qu'il sera jugé nécessaire aux fins de l'accord de service.

14- **Indemnisation et responsabilités**

14.1 Conformément à la section 14.2 ci-dessous, la société indemnisera le client des pertes, des dommages, des responsabilités, des actions, des jugements, des intérêts, des indemnités, des pénalités, des amendes, des

frais ou des dépenses, y compris des honoraires d'avocat raisonnables (« pertes »), directement liés ou directement conséquents à la réclamation d'un tiers contre le client qui est due ou liée à une infraction à la sécurité visant les données personnelles du client, à condition qu'il soit établi qu'il y a eu violation des clauses du programme de sécurité, en tout ou en partie, ou que l'infraction à la sécurité a été causée par une faille dans le programme de sécurité.

14.2 L'indemnisation décrite ci-dessus sera accordée à condition que le client : (a) avise promptement la société par écrit de la réclamation d'un tiers ; (b) accorde à la société le contrôle exclusif de la défense contre cette réclamation et de toute négociation de règlement connexe ; dans ce cas, la société n'aura pas l'autorisation de conclure un règlement ou d'accepter un compromis au nom du client sans le consentement préalable du client, consentement que le client ne devra pas refuser ou tarder à remettre sans motif raisonnable. Si la société n'assume pas la défense contre la réclamation d'un tiers, alors le client aura le droit d'assumer la défense contre cette réclamation en tant que seule partie défenderesse, étant entendu (i) qu'aucune disposition précédente ne limite ou n'est réputée limiter le droit d'une partie à contester le fait que la réclamation d'un tiers (et/ou les pertes en découlant) est liée à une infraction à la sécurité, et (ii) que, si la société a reconnu que la réclamation d'un tiers est liée à une infraction à la sécurité, le client n'a pas le pouvoir de conclure un règlement ou d'accepter un compromis au nom de la société sans l'autorisation de la société (autorisation que la société ne devra pas refuser ou tarder à remettre sans motif raisonnable). Dans tous les cas, le client aura le droit de participer à la défense lors d'une procédure judiciaire en choisissant son propre avocat, à ses frais, et devra collaborer avec la société pour se défendre contre la réclamation d'un tiers.

15- **Changements**

15.1 Si la société :

a) détermine qu'elle-même, un sous-traitant ultérieur, le centre de données, l'entité d'hébergement ou l'administrateur de système est incapable, à tout moment et pour quelque raison que ce soit, de se conformer aux obligations décrites dans les présentes CTD et ne peut remédier à cette incapacité de conformité ; ou

b) prend connaissance d'une circonstance ou d'un changement dans les lois applicables sur la protection des données personnelles qui peut compromettre considérablement la capacité de la société, d'un sous-traitant ultérieur, du centre de données, de l'entité d'hébergement ou de l'administrateur de système de respecter les obligations décrites dans les présentes CTD,

alors la société en informera promptement le client, qui, dans ce cas, aura le droit de suspendre temporairement le traitement des données personnelles du client jusqu'à ce que des modifications aient été apportées au traitement afin de remédier à la non-conformité.

16- **Évolution des CTD**

16.1 À la demande du client, la société et le client pourront de temps en temps évaluer le traitement des données personnelles du client. Si le client estime qu'il faut apporter des changements au traitement des données personnelles du client en vue d'assurer la conformité aux lois applicables sur la **protection des données personnelles**, alors le client et la société collaboreront afin d'évaluer les changements à apporter. La société informera le client de toute circonstance pouvant être pertinente à cet égard, y compris, mais sans s'y limiter :

1) les changements importants apportés à l'exécution de l'accord de service ; ou

2) les fusions, les réorganisations, la vente de la totalité ou presque des biens, les changements de contrôle ou d'effet des lois qui touchent la société, un sous-traitant ultérieur, le centre de données, l'entité d'hébergement ou l'administrateur de système.

Annexe 1 : programme de sécurité

Grands principes du programme de sécurité du groupe Gemalto

Préambule :

Ce document présente les éléments principaux du programme de sécurité du groupe Gemalto, qui assure la protection des données qui nous sont confiées.

Si les clients ont des questions ou désirent obtenir de plus amples renseignements, ils doivent communiquer avec leur représentant Gemalto, qui contactera ensuite le service de sécurité d'entreprise du groupe Gemalto au besoin.

Principes :

Le programme de sécurité permet d'assurer la protection dans le contexte actuel de nos activités internationales.

Notre programme de sécurité vise à :

a) déterminer, au moyen de l'analyse des risques, les menaces potentielles pour les renseignements des clients ;
b) mettre en place des solutions de sécurité (processus et outils) afin de limiter les risques pour nos systèmes ;
c) former nos employés et nos fournisseurs de service tiers afin de mettre en œuvre le programme de sécurité ;
d) surveiller la sécurité de nos systèmes et de nos processus ;
e) fournir des renseignements clairs quant au traitement des renseignements des clients ;
f) répondre aux demandes et aux requêtes des clients quant à la protection de leurs renseignements ;
g) nous préparer en cas de crise.

Les paragraphes suivants décrivent de façon plus détaillée les grands principes du programme de sécurité qui protège les renseignements des clients.

A- Grands principes

La gouvernance de notre programme de sécurité :

- est fondée sur plusieurs politiques applicables au groupe Gemalto ainsi qu'à tous les employés du groupe Gemalto, les employés des fournisseurs de service tiers et les personnes externes qui fournissent des services liés au système d'information (défini ci-dessous) ou ont recours à ce système ;

- relève de la responsabilité du service de sécurité d'entreprise et du service des TI, est géré localement par un responsable des TI et de la sécurité, et est assurée par des conseils de sécurité dont le fonctionnement est conforme à la norme ISO 27001 ;

- est révisée périodiquement ; son application est vérifiée au cours des vérifications de sécurité centrales et locales, et des vérifications de sécurité techniques sont effectuées à l'échelle locale et dans l'entreprise (la fréquence de ces vérifications varie selon le niveau de sécurité, de sensibilité et de vulnérabilité du système).

Notre programme de sécurité est axé sur les éléments suivants :

Identification et classification des renseignements personnels : la politique d'identification et de classification des renseignements personnels vise à établir un système de priorités pour la protection des renseignements et des biens afin d'assurer que les niveaux de protection sont proportionnés à la valeur des renseignements ou du système qui sont protégés tout au long de leur cycle de vie, de leur conception à leur destruction. L'utilisation de niveaux de classification permet à l'organisation de canaliser les ressources financières liées à la protection vers les renseignements ayant le plus de valeur. Cette politique traite des éléments principaux suivants :

- établir les règles d'entreprise du groupe Gemalto pour la gestion des renseignements en ce qui a trait à leur sensibilité ;
- déterminer la confidentialité des renseignements grâce à une méthode de classification à cinq niveaux, soit de « secrets » (niveau le plus élevé) à « publics » (niveau le plus bas) ;
- s'assurer que, à l'endroit où se trouvent les renseignements, la protection est en adéquation avec le niveau de classification des renseignements ;
- s'assurer que les restrictions d'accès logique aux ordinateurs et aux réseaux se font selon les mêmes règles que celles des restrictions d'accès physique ;
- veiller à ce que la réception des supports physiques contenant les renseignements confidentiels soit enregistrée ;
- établir les règles de transmission des renseignements ;
- établir les règles de stockage physique et électronique ainsi que de stockage des supports ;
- établir les règles visant la destruction ;
- établir la politique de rangement des documents.

Politique de sécurité environnementale et physique : pour protéger notre savoir-faire, il est essentiel d'établir les principaux moyens de défense contre le vol ou la mauvaise utilisation des produits et des services fournis par le groupe Gemalto. Ces moyens permettent aussi de protéger notre personnel. Cette politique traite des éléments principaux suivants :

- Elle s'applique à tous les sites du groupe Gemalto. Un site est un lieu physique, où les activités de Gemalto s'effectuent ou qui est un milieu de travail pour les employés du groupe Gemalto.
- Chaque site du groupe Gemalto doit respecter les caractéristiques de sécurité minimale ayant été définies, selon ses domaines d'activité et les risques déterminés pour ses processus.
- Chaque site du groupe Gemalto peut faire l'objet d'une vérification régulière de l'équipe de sécurité d'entreprise, qui vérifiera la conformité à la politique.
- Un responsable de la sécurité doit être affecté à chaque site du groupe Gemalto.
- Chaque site du groupe Gemalto est organisé en trois niveaux de zone, classés selon les services de sécurité qu'ils offrent.

Politique de sécurité des systèmes de gestion des configurations : cette politique vise à établir les règles de sécurité d'entreprise du groupe Gemalto quant à la gestion des logiciels pendant leur développement et jusqu'à leur livraison. Cette politique traite des éléments principaux suivants :

- les sujets principaux en matière de sécurité : confidentialité, intégrité, disponibilité, responsabilité et traçabilité ;
- la gestion des logiciels au moyen d'un outil informatique, appelé système de gestion des configurations (SGC) ;
- les conditions d'application à tous les employés, consultants ou entrepreneurs de Gemalto qui travaillent dans les installations de Gemalto ou qui se connectent à l'aide des réseaux ou d'un accès à distance ;
- la mise en œuvre de cette politique est vérifiée au cours des vérifications de sécurité centrales et locales ;
- en ce qui concerne l'application de cette politique, les rôles et les responsabilités sont distribués à un grand nombre d'employés de Gemalto, y compris du personnel de sécurité et du personnel qui participe au développement et à la gestion des logiciels ;
- les règles qui déterminent les restrictions d'accès au local où les logiciels sensibles sont conservés ;
- les règles qui régissent l'utilisation du cryptage pour assurer la confidentialité.

Plan d'assurance de sécurité pour le développement des logiciels : afin d'assurer une sécurité constante de bout en bout et de respecter les délais de mise en marché, nous définissons des « cibles de confiance ». Ce terme désigne l'exposition globale au risque en fonction du contexte du projet. Selon ces cibles, diverses activités de sécurité sont exécutées au cours du développement des logiciels. Ainsi, les activités de sécurité mises en place sont motivées par les risques auxquels nous sommes confrontés.

Cette quantification de la confiance peut s'effectuer avec le client en vue de mettre en évidence les principaux facteurs de risque.

Les activités réalisées pendant le développement des logiciels sont les suivantes :

- **Programme de formation** destiné aux équipes de développement.
- **Exigences de base :** exigences servant à établir un niveau de protection par défaut dans un logiciel. Selon l'évaluation des risques, d'autres contremesures peuvent être mises en œuvre en plus des exigences de base.
- **Gestion des risques :** identification, classification et traitement des risques principaux en fonction des cas d'utilisation et des logiciels de support.
- **Revue du code :** contrôles du code source (identification et correction des faiblesses fréquentes).
- **Évaluation de la vulnérabilité :** effectuée pendant et après le développement, elle sert à classer les vulnérabilités et peut entraîner le confinement et des mesures correctives.
- **Tests de la sécurité :** ils permettent d'assurer que chaque exigence liée à la sécurité est mise en œuvre et offre le niveau de protection attendu (portée du plan de test, tests d'applications dynamiques, tests d'intrusion).

Règles de sécurité pour la sous-traitance du développement des logiciels : en plus de la politique de sécurité des systèmes de gestion des configurations, le groupe Gemalto a établi une politique visant l'acquisition des services de tiers pour le développement de logiciels. La politique permet d'assurer la confidentialité des renseignements transmis au fournisseur de service. Cette politique traite des éléments principaux suivants :

- Définition de trois niveaux de sécurité afin d'établir un niveau de risque en fonction de la sensibilité du logiciel sur le plan de la sécurité. Le développement de logiciels ayant la sensibilité de sécurité la plus élevée (niveau 3) ne peut être sous-traité.
- La sous-traitance autorisée d'un logiciel doit faire l'objet d'un contrat qui impose l'utilisation de la norme ISO 27001 et des vérifications de sécurité.
- L'accès au réseau du groupe Gemalto fera l'objet d'une évaluation des risques, qui servira à définir les points de contrôle requis, les critères d'acceptation quant à la sécurité et l'affectation d'un représentant de la sécurité.
- Validation par le personnel de sécurité du groupe Gemalto des configurations logiques et physiques du fournisseur de service.
- Avant que le fournisseur de service ait accès aux renseignements, Gemalto doit avoir classé ces renseignements conformément à la politique d'identification et de classification des renseignements personnels. En fonction de cette classification, le fournisseur de service devra mettre en œuvre les règles applicables du groupe Gemalto.
- Les employés du fournisseur de service peuvent faire l'objet d'un contrôle de sécurité avant d'avoir accès aux renseignements. Seul un nombre minime d'employés peuvent avoir accès aux renseignements ; ils devront être formés quant au niveau de sécurité applicable.

Politique de sécurité du système d'information (« SI ») : cette politique a été définie conformément à la norme ISO 27001 afin de (a) souligner l'importance des principes de sécurité des SI pour les éléments stratégiques clés, comme les enjeux, le référentiel, les besoins en sécurité de l'entreprise et diverses menaces, et (b) assurer que nos exigences quant à la sécurité correspondent aux exigences de nos clients. Cette politique traite des éléments principaux suivants :

- Description des rôles et des responsabilités des employés du groupe Gemalto qui assurent la sécurité du système.
- La politique s'applique à tous les sites du groupe Gemalto, à tous les employés du groupe Gemalto et à tous les fournisseurs de service qui travaillent sur le SI du groupe Gemalto.
- Revue obligatoire de cette politique tous les deux ans.
- Définition des niveaux de sécurité pour déterminer les zones de sécurité applicables dans tous les sites de Gemalto.
- Les zones de sécurité définissent les règles de sécurité applicables en fonction de la sensibilité des renseignements traités.
- Définition des rôles et des responsabilités des employés du groupe Gemalto responsables d'assurer la mise en œuvre de la politique.
- Processus d'évaluation des risques.
- Conformité aux exigences réglementaires et juridiques dans les territoires où le groupe Gemalto exerce ses activités.
- Règles de sécurité applicables à l'utilisation de l'équipement mobile (par ex., ordinateur portable, tablette, téléphone mobile).
- Contrôle de l'accès dédié selon la classification de niveau de sécurité.
- Règles que doivent suivre toutes les personnes ayant accès au SI, y compris les fournisseurs de service tiers, afin d'assurer que le même niveau de sécurité est mis en œuvre.
- Principes de vérification qui définissent le processus de vérification applicable en fonction du niveau de sécurité applicable.
- Des tests d'intrusion de tiers sont mis en place avec les fournisseurs tiers.
- Contrôles de sécurité du SI à l'aide de coupe-feu, de détection des intrusions, de systèmes de prévention et de serveurs proxy Internet et intranet afin de protéger le SI des attaques extérieures.
- Protection contre les codes malveillants à l'aide de logiciels antivirus et de la détection des virus.
- Surveillance en temps réel pour bloquer les attaques extérieures contre notre SI.
- Étude sur la vulnérabilité de notre SI, qui peut déclencher le déploiement de correctifs de sécurité.
- Mise en œuvre d'un plan de reprise après sinistre dans les sites de Gemalto afin d'assurer la disponibilité du SI.

B- Équipe de gestion des incidents de sécurité informatique (EGISI) et programme de formation à la sécurité

Le groupe Gemalto a mis sur pied une organisation centralisée afin de renforcer la prévention et la protection contre les risques liés à la cybersécurité. Le fonctionnement de cette organisation est conforme à la norme RFC2350, qui décrit les attentes lors d'une intervention pour un incident de sécurité informatique, et est assuré par LEXSI, un CERT privé.

L'EGISI de Gemalto est composée de plusieurs experts des domaines de la cyberdéfense et des interventions en cas d'incident, ce qui comprend la criminalistique, les enquêtes sur les réseaux et les tests d'intrusion. La plupart de nos experts ont obtenu les certifications du GIAC (criminalistique) ou du Conseil européen (CEH) selon leurs responsabilités.

Chaque utilisateur du SI doit suivre une formation qui porte sur les pratiques de sécurité des systèmes d'information et qui est pertinente pour son utilisation des systèmes et des renseignements de Gemalto. Le contrôle des connaissances des utilisateurs fait l'objet d'un suivi.

Le service des ressources humaines est responsable de s'assurer que tous les nouveaux employés sont informés des principes de base quant à la sécurité des systèmes d'information. Les supérieurs directs sont responsables d'informer chaque employé des procédures, des normes et des politiques en matière de sécurité des systèmes d'information grâce à des programmes de sensibilisation. Les directeurs des services informatique sont responsables d'assurer la formation technique pertinente des membres de l'équipe des services informatique. Le service de la sécurité est responsable de la formation, de la certification et du suivi en ce qui concerne les pratiques de sécurité qui visent les systèmes d'information.

Annexe 2 : formulaire de traitement de données

La présente annexe décrit le service offert par les entités juridiques figurant dans ce document et qui sont responsables du traitement des données, ainsi que les types de données à traiter, les fins pour lesquelles les données sont traitées, la période pendant laquelle les données seront traitées à ces fins et les exigences obligatoires de rétention (s'il y a lieu).

Description des services :

[INDIQUER LE TYPE DE SERVICE À FOURNIR]

Le(s) client(s) est/sont :

[INDIQUER LE NOM DU OU DES CLIENTS]

Traitement des données :

[INDIQUER LA DESCRIPTION DU TRAITEMENT EFFECTUÉ PAR CHAQUE ENTREPRISE]

Ventilation des données : [REMPLIR LE TABLEAU]

	Type de données	Objectif	Période de rétention des données
1.			
2.			
3.			
4.			
5.			

Emplacement de l'entité d'hébergement ou du centre de données et identité de l'administrateur de système :

[INDIQUER L'EMPLACEMENT DE L'ÉQUIPEMENT DE TRAITEMENT, Y COMPRIS L'EMPLACEMENT DE L'ÉQUIPEMENT DE TRAITEMENT SERVANT À PRODUIRE LES RÉSULTATS STATISTIQUES]

Nom et emplacement du sous-traitant ultérieur qui assure les services de rapports aux fins de statistiques et de facturation.

[INDIQUER L'EMPLACEMENT DE L'ÉQUIPE QUI FOURNIT LES SERVICES DE RAPPORTS AUX FINS DE STATISTIQUES ET DE FACTURATION.]

Nom et emplacement du sous-traitant ultérieur qui assure les services de support.

[À REMPLIR]

Transmission des données par le client :

[DÉCRIRE LES MOYENS UTILISÉS POUR TRANSMETTRE LES DONNÉES AU(X) SOUS-TRAITANT(S) RESPONSABLE(S) DU TRAITEMENT DES DONNÉES. PAR EXEMPLE : Le client

utilise une voie de communication cryptée pour transmettre les données à des serveurs sécurisés, derrière le coupe-feu dédié de l'entité d'hébergement/du centre de données.]

Annexe 3 : termes relatifs au traitement de données dans le cadre des services de support technique

1. **Définitions**

Les termes suivants sont utilisés à la présente.

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

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.

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 ainsi que des communications 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.

2. **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.

3- **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 à l'emplacement indiqué à l'annexe 2 des CTD (formulaire de traitement de données).

Si Gemalto estime que la demande nécessite une connexion à distance à la solution, Gemalto accédera à la solution à l'aide d'un RPV sécurisé.

La connexion à distance permettant d'accéder à la solution est visée par les clauses relatives à la sécurité, décrites à la section 4 ci-dessous.

Lors de l'utilisation d'une connexion à distance pour accéder à la solution, 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.

4- **Clauses relatives à la sécurité**

4.1 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 :

4.1.1 Cloisonnement

Dans le but d'isoler la solution, 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 et l'équipe de support.

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 et l'équipe de support.

4.1.2 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. De plus, en fonction des définitions des rôles et des groupes, les droits d'accès sont limités à la prestation du service de support.

4.1.3 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- **Transfert transfrontalier**

5.1 Comme indiqué à la section 3 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 applicables 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.

5.2 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.