Politique de Traitement des Données à Caractère Personnel – STID Mobile ID®

STID accorde la plus grande importance à la protection de la vie privée des personnes. Toute information recueillie les concernant, lorsque vous avez décidé de les fournir, est destinée à nous permettre d'accomplir les prestations de services que vous nous avez confiées.

Les données personnelles recueillies par STID bénéficient de la protection de la loi "Informatique et Libertés" n° 78-17 du 6 janvier 1978 modifiée en 2004 et de celle du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. (Ci-après désignées par « Données personnelles »)

Toutes les données de nos clients restent circonscrites dans nos locaux et ceux de nos tiers de confiance cités ci-dessous. Seul le personnel ayant besoin de ces données dans le cadre de leur fonction ont un accès autorisé à vos Données personnelles. En outre, tous les employés sont informés des pratiques actualisées à respecter en matière de sécurité et de Données personnelles.

Dans le cadre de l'utilisation du service STID Mobile ID® nous sommes amenés à procéder à des traitements de Données personnelles vous concernant ainsi que des Utilisateurs tels que visés dans les CGU et celles de leurs salariés, clients et tiers. Toutefois, nous attirons votre attention sur le fait que ces Données personnelles étant chiffrées, STid n'a pas accès au contenu des informations chiffrées.

L'Utilisateur demeure responsable du traitement au sens de la réglementation applicable, des Données personnelles de ses salariés, clients et tiers qu'il peut mettre en œuvre dans le cadre de l'utilisation du service STID Mobile ID®.

Avant toute communication à STID de Données personnelles de vos salariés et/ou de tiers, vous devez au préalable avoir recueilli leur consentement tant pour les données collectées que pour les finalités envisagées. Le client garanti STID contre tous recours de ses salariés au titre des informations qui seront communiquées par le client à STID dans le cadre de l'utilisation du service STID Mobile ID®.

0.1 - Collecte des Données personnelles

Les Données à caractère personnel qui sont collectées sur ce site (ou « Plateforme ») sont les suivantes :

- Ouverture de Compte Utilisateur

Lors de la création du Compte de l'Utilisateur, la plateforme enregistre les données suivantes : civilité, nom, prénom, profession, numéro de téléphone fixe et mobile, numéro de fax, adresse électronique, nom, numéro d'immatriculation au RCS, numéro de TVA intracommunautaire, et numéro EORI des personnes physiques, nom du dirigeant, date de création, capital, profil (revendeur ou client final), site web de la société ainsi que la langue (Français, anglais) souhaité pour les échanges avec la société STid.

- Connexion

Lors de la connexion de l'Utilisateur à la Plateforme, celle-ci enregistre, notamment, son identifiant et son mot de passe.

- Profil

L'utilisation des prestations prévues sur la Plateforme permet de renseigner un profil, pouvant comprendre les données suivantes : logo, nom, prénom, e-mail et téléphone de l'utilisateur ainsi que toute donnée qu'il souhaite enregistrer (champs personnalisables), configuration rattachée au badge utilisateur, type d'ID utilisé (Private ou STid Mobile ID+) et photo de l'utilisateur.

- Cookies

La plateforme n'utilise pas de cookies traceurs.

Les cookies sont utilisés dans le cadre de l'utilisation du site. L'Utilisateur a la possibilité de désactiver les cookies à partir des paramètres de son navigateur.

Toutefois, la désactivation de certains cookies, risque de restreindre l'utilisation de certaines fonctionnalités du site.

Les cookies utilisés sur ce site sont les suivants :

- Cookie d'authentification
  Utilisé par le framework ASP.NET Identity (OWIN).
  Expire automatiquement après 24 heures (même si l'utilisateur travaille continuellement sur une application Web) et après 10 minutes d'inactivité.
  Sécurisé et nécessite SSL pour la communication.
  Cookie HttpOnly est activé, ce qui atténue le risque de création de scripts intersites. Attribut qui empêche l'accès aux cookies via le script côté client.

- Cookie de langue
  - Utilisé pour la traduction de la langue
    Non sécurisé dans lequel HttpOnly est désactivé.
    Sera initialisé la première fois que l'utilisateur ouvrira l'application Web.

0.2 - Utilisation et conservation des Données personnelles

Les Données personnelles collectées auprès des Utilisateurs ont pour objectif la mise à disposition des services de la Plateforme, leur amélioration et le maintien d'un environnement sécurisé.

Plus précisément, les utilisations sont les suivantes :

- accès et utilisation de la Plateforme par l'Utilisateur ;
- gestion du fonctionnement et optimisation de la Plateforme ;
- vérification, identification et authentification des données transmises par l'Utilisateur ;
- mise en œuvre d'une assistance Utilisateurs ;
-prévention et détection des fraudes, malwares (malicious softwares ou logiciels malveillants) et gestion des incidents de sécurité ;
- gestion des éventuels litiges avec les Utilisateurs ;
- celles telles que visées à l'article 0.7 ci-après dans le cadre des relations avec les sous-traitants

Les Données personnelles sont conservées tant que le compte est actif. Le compte est désactivé sur demande de l'Utilisateur ou lorsque de la dernière connexion au compte remonte à plus de trois ans.

0.3 - Partage des Données personnelles avec des tiers

Les Données personnelles peuvent être partagées avec des sociétés tierces, dans les cas suivants :

- si la loi l'exige, la Plateforme peut effectuer la transmission de données pour donner suite aux réclamations présentées contre la Plateforme et se conformer aux procédures administratives et judiciaires ;

- si la Plateforme est impliquée dans une opération de fusion, acquisition, de cession d'actifs ou procédure de redressement judiciaire, elle pourra être amenée à céder ou partager tout ou partie de ses actifs, y compris les Données à caractère personnel. Dans ce cas, le Responsable de traitement serait informé par STid avant tout transfert à une tierce partie, à charge pour le Responsable de traitement d'en informer les Utilisateurs pour leur permettre si besoin d'exercer leurs droits tels que visés au 0.5.

0.4- Sécurité et confidentialité

La Plateforme met en œuvre des mesures organisationnelles, techniques, logicielles et physiques en matière de sécurité numérique pour protéger les Données personnelles contre les altérations, destructions et accès non autorisés. Toutefois, II est à signaler que le Réseau Internet n'est pas un environnement complètement sécurisé et la Plateforme ne peut pas garantir la sécurité de la transmission ou du stockage des informations sur le Réseau Internet.

0.5 - Mise en œuvre des droits des Utilisateurs

En application de la réglementation applicable aux Données à caractère personnel les Utilisateurs peuvent mettre à jour, modifier ou supprimer les Données qui les concernent en se connectant à leur compte et en configurant les paramètres de ce Compte ;

Par ailleurs, en écrivant à l 'adresse électronique : dpo@stid.com des droits suivants :

- ils peuvent supprimer leur Compte, ou s'opposer au traitement de leurs Données personnelles,

- ils peuvent exercer leur droit d'accès, pour connaître les Données personnelles les concernant. Dans ce cas, avant la mise en œuvre de ce droit, STID peut demander une preuve de l'identité de la personne afin d'en vérifier l'exactitude,

- si les Données à caractère personnel détenues par la Plateforme sont inexactes, ils peuvent demander la mise à jour des informations,

- Ils peuvent demander la portabilité de leurs Données personnelles,

- Ils pourront déposer une réclamation auprès de la CNIL.

0.6. Evolution de la présente clause

La Plateforme se réserve le droit d'apporter toute modification à la présente clause relative à la protection des Données personnelles à tout moment. Si une modification est apportée la présente

clause de protection des Données personnelles la Plateforme s'engage à publier la nouvelle version sur la Plateforme. La Plateforme informera également les Utilisateurs de la modification par messagerie électronique, dans un délai minimum de 15 jours avant la date d'effet. Si l'Utilisateur n'est pas d'accord avec les termes de la nouvelle rédaction de la clause de protection des Données personnelles, celui-ci a la possibilité de demander la suppression de son Compte.

0.7. Relation avec les Sous-traitants au sens du RGPD

L'Utilisateur demeure responsable du traitement au sens de la réglementation applicable, des Données personnelles de ses clients et/ou employés, qu'il peut mettre en œuvre dans le cadre de l'utilisation des services.

Les Parties conviennent qu'au regard du Règlement européen sur la protection des Données personnelles :

Le **Responsable du traitement des données** est : L'Utilisateur

Le **Sous-traitant** : STid

Le **Sous-traitant de Rang 2** : La société Jaguar Network

Il est précisé que, compte tenu du chiffrement des Données, le Sous-traitant et le Sous-traitant de Rang 2 n'auront pas accès au détail des Données personnelles qui seront traitées par l'Utilisateur. En outre, la prestation du Sous-traitant déclinée au Sous-traitant de Rang 2 se limite eu égard aux Données personnelles, à fournir à l'Utilisateur un logiciel qui lui permette de saisir directement et de procéder lui-même au traitement des Données personnelles sans l'intervention du Sous-traitant ou du Sous-traitant de Rang 2.

Les données seront hébergées chez le Sous-traitant de Rang 2.

Les obligations qui suivent seront déclinées dans un acte séparé entre le Sous-traitant et le Sous-traitant de Rang 2, de manière que le Sous-Traitant puisse respecter l'ensemble des obligations contractées vis-à-vis du Responsable de Traitement.

Section I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable de traitement les opérations de traitement de Données personnelles définies ci-après.

Section II. Description du traitement faisant l'objet de la sous-traitance

Le Sous-traitant est autorisé à traiter pour le Compte du Responsable de traitement les Données et Données personnelles nécessaires pour fournir les besoins de l'utilisation de la Plateforme.

Gestion des données et Données personnelles RGPD

Hébergement des données chez STid ou chez le client

Création d'un compte rattaché à STid ou au client - Client final / Revendeur

			Données hébergées sur la plateforme SAAS Cloud STid			Données hébergées sur la platefome SAAS On Premise (chez le clie		
Données	**Type de Données**	**Finalité**	**STid**	**Cloud Jaguar Network**	**Client**	**STid**	**Client**	**Client du client**
Titre Mr / Mme	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme	Supervision Applicative & Sécurité 24x7x365 Sécurité des accès la plateforme Chiffrement de la base de données Mise en œuvre et exploitation de la plateforme Audit de sécurité Trimestriel Sauvegarde Externalisée Chiffrée	Stockage des données "brutes" de STid Disponibilité des données vers l'application Historisation des données de STid (Image VM 7 jours calendaires) Maintenance Niveau 1 - GTR Business 24x7x365 - Infogérance de l'OS + matériel Support client serveur 24h/24 7/7 via extranet client	Gestion des login / mots de passe Saisie des données personnelles	Fourniture des outils logiciels	Stockage des données Disponibilité des données Sauvegarde des données Maintenance Support client plateforme	Gestion des login / mots de passe Saisie des données personnelles
Prénom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Nom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Poste	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
N° de téléphone fixe	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
N° de téléphone portable	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Fax	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Email	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Nom société	Société	Enregistrement comptable						
N° de registration	Société	Enregistrement comptable						
N° de TVA	Société	Enregistrement comptable						
EORI	Société	Enregistrement comptable						
CEO	Société	Enregistrement comptable						
Date de fondation	Société	Enregistrement comptable						
Capital	Société	Enregistrement comptable						
Type de société revendeur ou client final	Société	Enregistrement comptable						
Pays	Société	Enregistrement comptable						
Adresse complète	Société	Enregistrement comptable						
Site Internet	Société	Enregistrement comptable						

Création d'un compte rattaché à sous-revendeur - Client final

Données	**Type de Données**	**Finalité**	**STid**	**Cloud Jaguar Network**	**Client**	**STid**	**Client**	**Client du client**
Nom société	Société	Permettre à l'utilisateur d'utiliser la plateforme	Supervision Applicative & Sécurité 24x7x365 Sécurité des accès la plateforme Chiffrement de la base de données Mise en œuvre et exploitation de la plateforme Audit de sécurité Trimestriel Sauvegarde Externalisée Chiffrée	Stockage des données "brutes" de STid Disponibilité des données vers l'application Historisation des données de STid (Image VM 7 jours calendaires) Maintenance Niveau 1 - GTR Business 24x7x365 - Infogérance de l'OS + matériel Support client serveur 24h/24 7/7 via extranet client	Gestion des login / mots de passe Saisie des données personnelles	Fourniture des outils logiciels	Stockage des données Disponibilité des données Sauvegarde des données Maintenance Support client plateforme	Gestion des login / mots de passe Saisie des données personnelles
Type de société revendeur ou client final	Société	Permettre à l'utilisateur d'utiliser la plateforme						
Catégorie tarifaire	Société	Permettre à l'utilisateur d'utiliser la plateforme						
Prénom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Nom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Email	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Téléphone	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Champs personnalisables par le client	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						

Création d'un site client

Données	**Type de Données**	**Finalité**	**STid**	**Cloud Jaguar Network**	**Client**	**STid**	**Client**	**Client du client**
Prénom utilisateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel	Supervision Applicative & Sécurité 24x7x365 Sécurité des accès la plateforme Chiffrement de la base de données Mise en œuvre et exploitation de la plateforme Audit de sécurité Trimestriel Sauvegarde Externalisée Chiffrée	Stockage des données "brutes" de STid Disponibilité des données vers l'application Historisation des données de STid (Image VM 7 jours calendaires) Maintenance Niveau 1 - GTR Business 24x7x365 - Infogérance de l'OS + matériel Support client serveur 24h/24 7/7 via extranet client	Gestion des login / mots de passe Saisie des données personnelles	Fourniture des outils logiciels	Stockage des données Disponibilité des données Sauvegarde des données Maintenance Support client plateforme	Gestion des login / mots de passe Saisie des données personnelles
Nom utilisateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel						
Configuration rattaché au badge utilisateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel						
Type ID : private ID ou STid Mobile ID+	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel						
Email utilisateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel						
Téléphone portable utilisateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge virtuel						
Champ variable sur l'utilisateur	Utilisateur	Permettre à l'utilisateur d'être identifié avec badge custom						
Photo de l'utilisateur	Utilisateur	Permettre à l'utilisateur d'être identifié avec badge custom						
Prénom configurateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge de configuration						
Nom configurateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge de configuration						
Email configurateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge de configuration						
Téléphone portable configurateur	Utilisateur	Permettre à l'utilisateur d'utiliser son badge de configuration						
Champ personnalisable par le client (configurateur)	Utilisateur	Permettre à l'utilisateur d'utiliser son badge de configuration						
Logo de la société	Société	Permettre à l'utilisateur d'être identifié avec badge custom						

Création d'un utilisateur de compte

Données	Type de Données	Finalité	STid	Datacenter Cloud Jaguar Network	Client	STid	Client	Client du client
Prénom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme	Supervision Applicative & Sécurité 24x7x365 Sécurité des accès la plateforme Chiffrement de la base de données Mise en œuvre et exploitation de la plateforme Audit de sécurité Trimestriel Sauvegarde Externalisée Chiffrée	Stockage des données "brutes" de STid Disponibilité des données vers l'application Historisation des données de STid (Image VM 7 jours calendaires) Maintenance Niveau 1 - GTR Business 24x7x365 - Infogérance de l'OS + matériel Support client serveur 24h/24 7/7 via extranet client	Gestion des login / mots de passe Saisie des données personnelles	Fourniture des outils logiciels	Stockage des données Disponibilité des données Sauvegarde des données Maintenance Support client plateforme	Gestion des login / mots de passe Saisie des données personnelles
Nom	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Email	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Téléphone	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						
Champs personnalisables par le client	Utilisateur	Permettre à l'utilisateur d'utiliser la plateforme						

Section III. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à :

1. traiter les Données personnelles **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance

2. traiter les Données personnelles **conformément aux instructions documentées** du Responsable de traitement figurant en annexe de la présente Annexe. Si le Sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des Données personnelles, il en **informe immédiatement** le Responsable de traitement. En outre, si le Sous-traitant est tenu de procéder à un transfert de Données personnelles vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public

3. garantir la **confidentialité** des Données personnelles traitées dans le cadre des CGU

4. veiller à ce que les **personnes autorisées à traiter les Données personnelles** en vertu des CGU :

- s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
- reçoivent la **formation** nécessaire en matière de protection des Données personnelles

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des Données personnelles dès la conception** et de **protection des Données personnelles par défaut**

6. Sous-traitance

Le Sous-traitant peut faire appel à un autre Sous-traitant de Rang 2 (ci-après, « ***le Sous-traitant de Rang 2 ultérieur*** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant et les dates du contrat de sous-traitance. Le Responsable de traitement dispose d'un délai minium de 8 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le Sous-traitant de Rang 2 ultérieur est tenu de respecter les obligations des CGU pour le compte et selon les instructions du Responsable de traitement. Il appartient au Sous-traitant de Rang 2 initial de s'assurer que le Sous-traitant de Rang 2 ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du règlement européen sur la protection des Données personnelles. Si le Sous-traitant de Rang 2 ultérieur ne remplit pas ses obligations en matière de protection des Données personnelles, le Sous-traitant de Rang 2 initial demeure pleinement responsable devant le Responsable de traitement de l'exécution par l'autre Sous-traitant de Rang 2 de ses obligations.

7. Droit d'information des personnes concernées

Il appartient au Responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des Données personnelles.

8. Exercice des droits des personnes

Les données étant chiffrées, par voie de conséquence le Sous-traitant n'ayant pas accès au contenu des données, il appartiendra au Responsable de traitement de s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des Données personnelles, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d'exercice de leurs droits, le Sous-traitant adressera ces demandes au Responsable de traitement.

9. Notification des violations de Données personnelles

Le Sous-traitant notifie au Responsable de traitement toute violation de Données personnelles dans un délai maximum de 24 heures après en avoir pris connaissance et par e-mail. Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10. Aide du Sous-traitant dans le cadre du respect par le Responsable de traitement de ses obligations

Le Sous-traitant aide le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des Données personnelles.

Le Sous-traitant aide le Responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

Contrôle d'accès physique : chez Jaguar Network.

Contrôle d'accès logique : l'accès à la plateforme (serveurs) en mode administrateur n'est possible qu'après une authentification Windows d'un pool d'IP autorisé. Cette authentification est totalement décorrélée de celle qui permet l'accès à la base de données.

Décomposition des rôles fonctionnels de la solution STid Mobile ID : chaque rôle a ses propres accès (cloisonnement). Aucun partage d'informations et de connaissances entre :

Administrateur du serveur / administrateur de la base de données / administrateur du chiffrement de la base de données / administrateur de chaque compte Revendeur / Utilisateur final.

Seules les personnes authentifiées peuvent lire/modifier/effacer des données à caractère personnel selon les droits qui leurs sont attribués.

Personnalisation des clés de protection pour chaque entité (un Revendeur/sous-revendeur peut uniquement accéder à son compte, et possède son propre jeu de clés de protection).

Décomposition des rôles de gestions de la base de données, l'administrateur n'a pas connaissance des clés de protections de chaque revendeur et ne peut pas interpréter les données gérées par la base de données, et le gestionnaire de la base de données n'a pas connaissance de la clé maître de la base de données.

Toutes les données utilisateurs sont signées, et authentifiées, ce qui permet de se prémunir de la corruption et de la falsification.

La disponibilité de ces données est fonction des SLA de Jaguar Network.

Le temps de rétablissement d'accès à ces données est aussi fonction du SLA de Jaguar Network, et selon l'historisation des serveurs.

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces Données personnelles, le Sous-traitant s'engage à :

- détruire toutes les Données personnelles ou
- à renvoyer toutes les Données personnelles au Responsable de traitement ou
- à renvoyer les Données personnelles au Sous-traitant désigné par le Responsable de traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-traitant. Une fois détruites, le Sous-traitant doit justifier par écrit de la destruction.

13. Délégué à la protection des Données personnelles

Le Sous-traitant communique au Responsable de traitement **le nom et les coordonnées de son délégué à la protection des Données personnelles**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des Données personnelles.

14. Registre des catégories d'activités de traitement

Le Sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement comprenant :

- le nom et les coordonnées du Responsable de traitement pour le compte duquel il agit, des éventuels Sous-traitants et, le cas échéant, du délégué à la protection des Données personnelles ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de Données personnelles vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des Données personnelles, les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

    - la pseudonymisation et le chiffrement des Données personnelles;
    - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

- des moyens permettant de rétablir la disponibilité des Données personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Documentation

Le Sous-traitant met à la disposition du Responsable de traitement la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Section IV. Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à :

1. fournir au Sous-traitant les données visées au II des présentes clauses,

2. documenter par écrit toute instruction concernant le traitement des Données personnelles par le Sous-traitant,

3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des Données personnelles de la part du Sous-traitant,

4. superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.