Politique de gestion des données à caractère personnel

Version:	1.0
Date de la version:	18/05/2018
Créé par:	Bruce GARNIER
Approuvée par:	Philippe GANGNEUX, Olivier NOVASQUE
Niveau de confidentialité:	Public

Historique des modifications

Date	Version	Créé par	Description de la modification
18/05/2018	0.1	Bruce GARNIER	Création

Table des matières

I. Contexte

Dans le cadre du Règlement général sur la protection des données (RGPD), Sidetrade s'engage à respecter les principes de protection des données personnelles des personnes concernées (utilisateurs, collaborateurs, tiers, etc.) collectées et utilisées dans le cadre de leur activité.

I.1 Objectifs

Cette politique sur la protection des données à caractère personnel définit les principes directeurs à mettre en place au sein de Sidetrade, notamment au regard des exigences du règlement européen général sur la protection des données à caractère personnel (GDPR ou RGPD).

Ces principes directeurs devront permettre d'établir les procédures nécessaires et adéquates au contexte de Sidetrade afin de répondre aux exigences suivantes :

- Déterminer un référentiel d'exigences en matière de protection des données afin de répondre aux engagements de Sidetrade
- Sensibiliser l'organisation, le personnel et les contractuels (employés à plein temps, temps partiel, entrepreneurs, équipes internes, intérimaires et autres personnes engagées par Sidetrade), à moins que cela ne contrevienne à des règlementations locales en vigueur dans le contexte de l'organisation
- Soutenir les opérations métiers en cours pour répondre aux normes de protection des données adéquates
- Se conformer aux règlementations applicables telles que le GDPR et autres lois nationales

I.2 Périmètre

Toutes les filiales de Sidetrade en France et à l'internationale sont tenues de respecter cette politique et de traiter les données personnelles conformément au GDPR et/ou à la règlementation applicable selon les principes décrits dans ce document.

Cette politique est communiquée à tous les collaborateurs de Sidetrade. L'emplacement de la version de référence est précisé en annexe.

Certains principes de la politique s'appliquent également aux tiers en relation avec Sidetrade. Ces informations sont précisées dans un chapitre prévu à cet effet.

I.3 Dérogations

Toute dérogation à cette politique doit être documentée et motivée par son demandeur, et validée formellement par le Délégué de la Protection des Données de Sidetrade (ou Data Protection Officer – DPO).

En particulier, si certaines dispositions contreviennent à des lois ou règlementations locales en vigueur, une dérogation peut être prononcée et des règles complémentaires peuvent s'y substituer afin de maintenir un niveau adéquat de protection des données personnelles.

I.4 Suivi documentaire

La Politique de protection des données personnelles est révisée au plus tous les trois ans par le Délégué de la Protection des Données de Sidetrade, notamment lors de changements législatifs ayant un potentiel impact sur la gestion des données personnelles.

Avant publication cette politique doit être validée par la direction juridique.

A chaque mise à jour du document, cette politique est diffusée dans l'ensemble des filiales Sidetrade.

II. Gouvernance et responsabilités des parties prenantes

Cette politique est d'application globale à Sidetrade. Les filiales pour chaque Pays peuvent choisir d'implémenter cette politique directement ou bien de l'adapter, à condition que la politique locale reste alignée avec les principes décrits dans la politique principale Sidetrade.

Les parties prenantes décrites ci- après représente le dispositif de conformité

II.1 Direction générale et COMEX

La Direction Générale est responsable de l'application, du respect de cette politique et de la conformité aux exigences réglementaires applicables.

Elle s'assure que des ressources suffisantes soient disponibles pour atteindre et maintenir la mise en conformité de Sidetrade, dans chacune des filiales concernées.

Aussi, afin d'assurer la cohérence et le suivi des actions de mise en œuvre et du maintien du dispositif de conformité, la Direction Générale doit disposer d'une visibilité sur les actions entreprises et leur suivi. Cette vision est fournie par le DPO (voir description ci après)

Le DPO assure une intervention annuelle auprès du Comité Exécutif Groupe, afin de :

- Valider le budget alloué à la protection des données
- Présenter les chantiers prioritaires identifiés en matière de protection des données et l'avancement de Sidetrade sur ces chantiers
- Faire part de son bilan pour l'année écoulée : faits marquants, points d'attention et besoins d'arbitrage.

En particulier, le DPO informe la Direction Générale sur tous les développements (organisationnels, réglementaires…) susceptibles d'avoir une incidence sur la protection des données.

II.2 Rôles et responsabilités du Délégué à la Protection des Données (ou *Data Protection Officer* « DPO »)

Le « Délégué à la protection des données » ou DPO est chargé de contrôler et suivre le développement de la mise en œuvre de la politique des données personnelles de Sidetrade.

Il favorise le transfert de connaissances entre les filiales locales afin d'améliorer le programme de conformité de Sidetrade et de favoriser une approche cohérente avec les objectifs du programme tout en respectant les exigences légales spécifiques à Sidetrade.

Le DPO est le point de contact avec les autorités de contrôle en matière de protection des données à caractère personnel. Il est chargé de liaison et de la coopération avec les autorités de contrôle en cas de besoin.

Ses missions sont les suivantes :

- Mettre en place une gouvernance de protection des données et l'animer
- Sensibiliser, conseiller et assister
- Représenter, consulter et coopérer
- Piloter et conduire des programmes et projets relatifs à la protection de la vie privée
- Évaluer, contrôler et préconiser
- Conduire la veille autour de la protection des données personnelles

Des informations supplémentaires sur l'ensemble des missions du DPO sont disponibles dans la fiche de poste du DPO.

II.3 Rôles et responsabilités des équipes opérationnelles (métiers et IT)

Les directions métiers sont responsables, sur le périmètre de leur activité, du respect de la règlementation en vigueur et de la présente politique.

En particulier, elles sont responsables, sur leur périmètre d'activité :

- De l'identification et du maintien de la documentation des traitements de DCP et de leur périmètre respectif ;
- De l'intégration des principes de protection de la vie privée par conception et par défaut dans leurs activités et en particulier dans le développement de leurs projets ;
- De la réalisation d'études d'impacts sur la vie privée sur les traitements de données à caractère personnel qui le nécessitent ;
- De relayer les demandes de droits des personnes concernées aux équipes pertinentes ;
- D'alerter le DPO au plus tôt en cas de suspicion de violation de données à caractère personnel.

Dans ce cadre, elles peuvent solliciter l'avis et les conseils du DPO dans la réalisation de ces missions.

II.4 Correspondants vie privée dans les Métiers et les Pays

Un correspondant vie privée est nommé au minimum pour chacune des filiales européennes du groupe Sidetrade. A défaut d'un correspondant formellement nommé, le responsable de la filiale assume ce rôle.

Le correspondant vie privée est en charge sur son périmètre de :

- Décliner localement si nécessaire les principes et règles de protection de la vie privée, de manière coordonnée avec le DPO.
- Contrôler la bonne mise en place des règles de protection de la vie privée du groupe Sidetrade ou de leur déclinaison locale
- Constituer un relai de proximité pour les questions relatives à la protection de la vie privée et le respect du GDPR

II.5 Direction des systèmes d'information

La direction des systèmes d'information a un rôle de support au Délégué à la Protection des Données, notamment dans le cadre de son expertise IT et en particulier, dans ses connaissances de la sécurité des systèmes d'information Sidetrade.

C'est un acteur clé dans le projet de mise en conformité GDPR au vu des mesures la protection des données personnelles relatives à la sécurité des systèmes d'information. Elle jouera un rôle essentiel notamment pour les sujets de gestion de rétention des données personnelles, du respect des droits des personnes, des analyses d'impacts sur la vie privée ainsi que sur les mesures techniques et opérationnelles de protection et sécurisation des données personnelles.

II.6 Direction Juridique

La Direction juridique a un rôle clé vis-à-vis de la Protection des Données, notamment dans le cadre de son expertise IT et en particulier, dans ses connaissances de la règlementation GDPR et des autres règlementations spécifiques à l'activité de Sidetrade.

Elle joue un rôle essentiel notamment pour les sujets de gestion des tiers (ie : sous-traitant, clients,…) et de revue contractuelle associée, des bases légales et gestion des consentements, mais aussi des aspects contractuels des collaborateurs. A défaut de disposer d'une direction juridique les aspects de la gestion tiers seront pris en charge par la direction administrative et financière, ceux des collaborateurs et des candidats par la direction des ressources humaines, ceux des prospections clientes par la direction de la communication.

II.7 Comité protection de la vie privée

Ce comité est dédié au suivi et à la réalisation opérationnelle de la protection de la vie privée. Il est assuré à minima une fois par semestre et est constitué des personnes suivantes :

- Le Président Directeur Général (présidence du comité)
- Le Délégué à la Protection des Données
- Le Directeur Juridique ou ces représentants nommés
- Les correspondants vie privée des Métiers et Pays

Ce comité a pour objectif de :

- Présenter et assurer le suivi des principaux indicateurs de conformité au RGPD au niveau organisationnel, Métiers et Pays.
- Déterminer et prioriser les chantiers importants en matière de protection des données
- Remonter les informations sur les problématiques de protection de la vie privée rencontrées chez Sidetrade (audits de contrôle, violations de données, plaintes de personnes concernées, etc.).

III. Principes de protection de la vie privée

III.1 Définitions

Pour les besoins de la présente politique, les définitions suivantes s'appliquent :

- « Données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; Les « catégories particulières de données personnelles » désignent toute donnée personnelle révélatrice d'origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques, données de santé ou données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

- « Personne concernée » (« *data subject* » en anglais) est la personne physique qui fait l'objet des « Données Personnelles » et est identifiée ou identifiable, directement ou indirectement

- « Sous-traitants ou Tiers » (« data processor » en anglais) est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui **traite des données à caractère personnel** pour le compte du responsable du traitement

Par la

- « Responsable du traitement » (*« data controler* » en anglais) correspond à la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque deux ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens de traitement, ils sont appelés « responsables conjoints »

- «Traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

- « Destinataire », la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires. Le traitement de ces données par les autorités publiques en

question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement

- « *Privacy By design/by default*», le fait de garantir la protection des données à caractère personnel traitées par défaut et avant la conception de nouveau service/traitement/produit .

III.2 Principes de protection de la vie privée (Principe d'« *Accountability* »)

L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Plus précisément, Sidetrade se doit de respecter les exigences suivantes :

- Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques […] pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

- Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au point précédent comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

- L'application d'un code de conduite approuvé […] peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Les principes de protection des données personnelles suivants doivent être respectés et Sidetrade doit être en capacité d'apporter les preuves de leur respect :

- **Responsabilité :** Pour chaque traitement de données à caractère personnel, un collaborateur Sidetrade en charge du traitement est formellement identifié. A défaut, le CEO ou CTO de la filiale est considéré comme étant en responsable du traitement. Le collaborateur en charge est responsable du respect de la politique de protection des données personnelles pour les traitements dont il a la charge. Il est en mesure de démontrer que celle-ci est respectée
- **Licéité, loyauté et transparence** : les données à caractère personnel sont traitées de manière licite, loyale et transparente au regard de la personne concernée
- **Finalités déterminées** : Les données à caractère personnel ne sont collectées uniquement pour la réalisation d'opérations dont les finalités/objectifs sont déterminés
- **Intégrité et confidentialité** : les données à caractère personnel sont traitées de façon à garantir leur sécurité à l'aide de mesures techniques ou organisationnelles appropriées
- **Exactitude** : les données à caractère personnel restent exactes et, si nécessaire, tenues à jour;
- **Minimisation des données** : les données à caractère personnel collectées, stockées, échangées et manipulées sont systématiquement limitées aux données adéquates,

pertinentes et restreintes à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

- **Limitation de la conservation** : les données à caractère personnel ne sont pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités du traitement pour lesquelles elles sont traitées

De ces principes en découlent des règles de protection de la vie privée (Règles d' « *Accountability* »)

IV. Règles de protection de la vie privée (Règles d'« *Accountability* »)

Afin de respecter les engagements sur les principes de protection des données les règles ci-après sont définies.

Elles visent notamment à garantir la capacité de Sidetrade à apporter les preuves de sa bonne conformité au Règlement.

Les règles édictées dans cette politique constituent la pratique minimale requise.

Le DPO contrôle que cette politique est mise en œuvre de manière appropriée au sein de Sidetrade, sous la responsabilité de la direction générale. La mise en œuvre de cette politique est menée et supervisée conjointement avec tout dispositif de conformité local.

IV.1 Gouvernance de la protection des données

IV.1.1 Organisation

Les filiales de Sidetrade mettent en place des procédures claires pour garantir le respect des principes et des règles de cette politique. Elles s'assurent de leur respect par des procédures de contrôle adaptées.

Chaque filiale de Sidetrade est responsable de réaliser annuellement une analyse des écarts à la politique de protection des données personnelles, et de la communiquer au Délégué à la Protection des Données, accompagnée du plan d'actions prévu pour combler les écarts constatés.

IV.1.2 Responsabilité du traitement

Afin de comprendre et de respecter les exigences règlementaires sur la protection des données personnelles, il est essentiel d'identifier la position de Sidetrade en ce qui concerne les traitements des données personnelles.

On distingue Sidetrade sous trois positions suivant les traitements :

- Responsable de traitement
- Responsable conjoint de traitement
- Sous-traitant

Pour rappel le sous-traitant est soumis aux exigences suivantes :

- Compte tenu de la nature du traitement, le sous-traitant se doit d'aider le responsable de traitement, dans la mesure du possible, dans le cadre de l'obligation de réponse aux droits des personnes, notamment par des mesures techniques et organisationnelles appropriées.
- Aider le responsable du traitement des données à garantir le respect des obligations relatives à la sécurité des données personnelles (en tenant compte de la nature du traitement et des informations mises à la disposition du responsable de traitement)
- Mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer sa conformité avec le GDPR, permettre et contribuer à l'obligation de contrôle auquel est soumis le responsable de traitement, y compris les dans le cas d'inspections menées par le responsable de traitement ou un autre auditeur mandaté par le responsable de traitement.

IV.1.3 Relation avec l'autorité de contrôle

Le DPO est en charge des relations de Sidetrade avec les autorités de contrôle (CNIL pour la France), en coopération avec la direction de la communication.

Le DPO est informé de toute prise de contact de la part d'une autorité de contrôle.

Sidetrade coopère avec les autorités de contrôle. Cette coopération se traduit par plusieurs actions :

- La notification à l'autorité de contrôle en cas de violation de données, conformément aux dispositions de la procédure de gestion des violations de données personnelles.
- La mise à disposition de toute documentation justifiant du respect de la mise en conformité à la demande de l'autorité, coordonnée par le DPO.

IV.2 Registre des traitements

Sidetrade maintient un registre des activités de traitements des données à caractère personnel, contenant les caractéristiques descriptives du traitement.

Le registre est renseigné et tenu à jour par les personnes en charge de chacun des traitements.

Le DPO est garant du registre des traitements des données personnelles de Sidetrade et de son maintien. A ce titre, il s'assure de sa bonne mise à jour par les personnes en charge des traitements.

Chaque traitement dans le registre est revu au minimum une fois par an par la personne en charge du traitement.

IV.3 Sécurité des traitements

Sidetrade s'assure d'un niveau adéquat de sécurité des traitements sur les données à caractère personnel effectués.

Les activités de traitement bénéficient d'un niveau de sécurité adapté aux risques qu'ils sont susceptibles de faire courir aux personnes concernées.

Ces données personnelles doivent être protégées au minimum comme toutes les autres données traitées ou détenues par les entités de Sidetrade et conformément à la présente politique.

Pour cela, des mesures techniques de contrôle doivent être mises en place, ces mesures en accord avec la gestion du risque doivent permettre (à titre d'exemple) :

- **Contrôle d'accès** : permet d'empêcher des personnes non autorisées d'accéder à des systèmes où des données personnelles sont stockées, à des fins de traitement ou d'utilisation des données personnelles du client ;
- **Contrôle d'accès** : Les personnes autorisées à utiliser un système de traitement de données n'ont accès qu'aux données personnelles auxquelles elles sont autorisées à accéder, et les données personnelles ne **peuvent être lues, copiées, altérées ou retirées sans autorisation** pendant le traitement, l'utilisation et après l'enregistrement ;
- **Contrôle de la divulgation** : Les données personnelles ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le transfert ou le transport électronique ou pendant leur enregistrement sur un support de données, et il est possible de vérifier les personnes ayant le droit de transférer
- **Contrôle d'entrée** : Il est possible de vérifier si les données personnelles ont été consultées, modifiées ou retirées des systèmes de traitement de données et, dans l'affirmative, par qui ;
- **Contrôle du travail effectué** : Les données personnelles traitées pour le compte d'autrui sont traitées strictement en conformité avec les responsabilités professionnelles des personnes accédant aux données personnelles
- **Contrôle de disponibilité** : Les données personnelles sont protégées contre la destruction ou la perte accidentelle
- **Politique du bureau propre** : Aucune donnée personnelle ne doit être laissée dans un endroit facilement visible ou accessible lorsqu'elle n'est pas utilisée et les responsables de traitement. Ces données personnelles doivent être archivées et stockées correctement et en toute sécurité lorsqu'elles ne sont pas utilisées
- Des accords de confidentialité ou des clauses de confidentialité dans les accords contractuels doivent être mis en place pour toutes les tierces parties avec lesquelles Sidetrade interagit
- Les employés et autres parties doivent être vigilants lors de leurs déplacements et lors de leur travail en dehors des locaux de l'entreprise. Les données personnelles ne doivent pas être divulguées dans des lieux publics. Des précautions appropriées doivent être prises si des données personnelles sont contenues sur les supports de Sidetrade comme les ordinateurs portables, les téléphones mobiles, etc
- Une sauvegarde appropriée des données personnelles du système doit être effectuée régulièrement

- La distribution de données personnelles à toute entité extérieure à Sidetrade est **strictement interdite**, excepté à des tiers désignés par des clients ou par Sidetrade, et **agissant dans la capacité pour laquelle ils ont été désignés**, et conformément aux lois locales applicables. Toute exception à cette règle ne peut être envisagée que si une entité de Sidetrade est obligée de fournir des informations à une autre partie pour des raisons légales et/ou réglementaires. Dans ce cas, la distribution ou le transfert doit être autorisé par le responsable local de la protection des données
- Dans les situations où des données personnelles sont également considérées comme des informations privilégiées, la politique sur les délits d'initiés et les abus de marché s'applique.

Aucune donnée personnelle ne doit être dans des environnements informatiques considérés comme « hors production » (tels que les environnements de développement et de test).

Si cela n'est pas possible, le DPO doit être informé de la nécessité de traiter les données à caractère personnel dans un environnement hors production et une analyse doit être effectuée pour s'assurer que les garanties appropriées ont été mises en œuvre. – cad : bénéficier d'un niveau de sécurité adapté à leur besoin de sécurité (confidentialité, anonymisation et gestion des accès, …).

Toutes les activités de traitement doivent être consignées dans le registre, y compris le traitement effectué dans un environnement hors production.

IV.4 Cycle de vie des données

IV.4.1 Information préalable

Lorsque des données à caractère personnel sont collectées, le responsable du traitement est tenu de fournir à la personne concernée, au moment où les données en question sont obtenues, les informations sur la **collecte**, **la finalité** et **l'utilisation** de ces données, en conformité avec le principe de **transparence**.

Ces informations sont fournies par le responsable du traitement à la personne concernée au moment de la collecte, ou dans un délai raisonnable après l'obtention des données personnelles si elles ne sont pas directement collectées auprès de la personne concernée.

Les obligations d'information ci-dessus ne s'appliquent pas si la personne concernée :

- dispose **déjà des informations ou si la fourniture de ces informations s'avère impossible ou impliquerait un effort disproportionné**. Dans ce cas, des mesures appropriées pour protéger les droits et libertés du sujet de données sont prises, y compris en rendant l'information accessible au public.

IV.4.2 Gestion de la collecte des données

Base légale

Les données personnelles doivent être obtenues **équitablement et légalement**, c'est pourquoi il existe 6 bases légales possibles pour un traitement de données à caractère personnel :

- Les personnes concernées ont **donné leur consentement** au traitement de leurs données personnelles pour une ou plusieurs finalités spécifiques
- Le traitement est nécessaire pour **l'exécution d'un contrat** auquel la personne concernée est partie, ou pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat
- Le traitement est nécessaire pour le respect d'une **obligation légale** d'un pays de l'Union Européenne à laquelle Sidetrade est soumis
- Le traitement est nécessaire pour protéger **l'intérêt vital** de la personne concernée ou d'une autre personne physique
- Le traitement est nécessaire à **l'exécution d'une tâche effectuée dans l'intérêt public** ou dans l'exercice de l'autorité publique dévolue au responsable du traitement des données
- Le traitement est nécessaire **aux fins des intérêts légitimes** poursuivis par le responsable du traitement des données ou par un tiers, sauf si ces intérêts sont outrepassés par l'intérêt ou les droits fondamentaux et la liberté des personnes concernées (en particulier lorsque les est un enfant). L'utilisation de cette base comme base juridique pour le traitement doit être validée par la direction juridique

La base légale pour le traitement doit être documenté et justifié, par exemple en citant l'article de loi qui impose une obligation légale, ou avec une évaluation documentée d'intérêt légitime.

Classification des données personnelles

Les données personnelles ont été divisées en **3 catégories en fonction de leur sensibilité** pour les personnes concernées

Les catégories sont les suivantes :

Classification	Description	Principes
Personnel – professionnel	Les données personnelles qui sont des informations de **contact professionnelles** (*exemples : le nom, le titre du poste, l'adresse e-mail professionnelle ou le numéro de téléphone professionnel*)	-
Personnel – standard	Les données personnelles des personnes, **en dehors d'un contexte professionnel** (*exemples : l'adresse personnelle, l'adresse électronique personnelle, le sexe, le nombre d'enfants, habitudes de vie, etc.*)	-
Personnel - sensible	Cette catégorie comprend des catégories particulières de données à caractère personnel telles que origine raciale ou ethnique, opinions politiques, croyances	L'utilisation de ces données est strictement interdite, sauf si l'une des conditions sauf exceptions (décrites dans

	religieuses ou philosophiques, appartenance syndicale, données génétiques, biométriques, liées à la santé, vie sexuelle, infractions pénales et condamnations pénales, ainsi que les documents et identifiants officiels (cartes d'identité, permis de conduire, passeport, numéro de sécurité sociale).	l'article 9 et 10 du GDPR)

Consentement

Dans le cas de certains traitements sur les données à caractère personnel, le consentement préalable des personnes est nécessaire. Dans ce cas, Sidetrade doit être en mesure de démontrer que les personnes concernées ont donné leur consentement à l'utilisation de leurs données personnelles.

Le consentement doit être donné « par un acte positif clair » par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données la concernant.

La personne concernée est en mesure de retirer son consentement de manière aussi simple que celui-ci a été donné.

Lorsque que le traitement a plusieurs finalités, le consentement doit être demandé pour **chacune** des finalités de celui-ci.

Afin d'assurer sa capacité à faire valoir de sa bonne conformité, Sidetrade est en mesure de tracer les consentements donnés et retirés.

Le consentement de la personne concernée est défini comme « toute manifestation de v**olonté, libre, spécifique, éclairée et univoque** par laquelle la personne concernée accepte, par une déclaration ou par un **acte positif clair**, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Il peut être donné par la une déclaration écrite, y compris par la voie électronique, mais aussi par une déclaration orale. Si le consentement du sujet de données doit être donné suite à une demande par voie électronique, la demande doit être **claire, concise et ne pas perturber inutilement** l'utilisation du service pour lequel elle est fournie.

L'absence de consentement, les cases-pré-cochées ou encore l'inactivité ne constitue par un consentement.

IV.4.3 Gestion de l'exercice des droits

Sidetrade est tenu de respecter l'exercice des droits des personnes concernées, à savoir :

- Transparence

- Droit à l'information
- Droit d'accès
- Droit de rectification
- Droit à l'oubli
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d'opposition au traitement

La manière dont les personnes concernées peuvent contacter Sidetrade pour faire valoir leur droit est précisée dans l'information préalable des personnes concernées.

Les demandes des personnes concernées sont analysées et instruites dans un délai raisonnable.

Les personnes concernées sont informées sous un mois de la suite donnée à leur demande.

La gestion de l'exercice des droits est détaillée dans **la procédure de gestion des droits des personnes**.

IV.4.4 Gestion de la durée de rétention

Les données personnelles ne sont pas conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été obtenues ou enregistrées, ou pour une durée supérieure à celle requise par les exigences réglementaires applicables.

La durée de conservation des données à caractère personnel est portée dans le registre de traitements des données à caractère personnel.

Lorsque les données personnelles sont conservées, des **informations appropriées, le stockage, l'archivage, la propriété et la classification** des données personnelles doivent être mis en place pour sécuriser et protéger les données personnelles conformément aux durées de conservation définies par Sidetrade (plus précisément par le département juridique).

Les données personnelles doivent être effacées ou rendues anonymes lorsqu'il n'est plus nécessaire de les conserver aux fins pour lesquelles elles ont été obtenues ou enregistrées ou pour les exigences légales ou réglementaires applicables.

La procédure de conservation des données doit être évaluée par rapport à la réglementation locale applicable.

IV.5 Gestion de la vie privée dans les projets

IV.5.1 Minimisation des données

De manière générale, seules les données personnelles nécessaires au bon fonctionnement des traitements sont collectées, stockées, utilisées, transmises et accédées.

Pour tout changement de finalités du traitement des données personnelles, il est tenu de vérifier la nécessité des données personnelles collectées.

*NB : Les données personnelles **ne peuvent être vendues à des tiers,** sauf si la loi l'exige ou si le consentement de la personne concernée a été obtenu.*

IV.5.2 Gestion des accès

Les accès aux données personnelles doivent être maîtrisés de manière à ce que seules les personnes ayant à manipuler ces données dans le cadre de leur mission soient en mesure de le faire.

En particulier, l'accès aux données à caractère personnel dans les systèmes d'information est conditionné à l'authentification et à l'habilitation de l'utilisateur.

La gestion des accès est maîtrisée, notamment par une gestion des arrivées/départs/mobilités, ainsi que par une revue régulière des accès.

Pour toute documentation papier existante incluant des données personnelles, il convient de les stocker dans des espaces sécurisés, de manière à pouvoir y accéder sur besoin par les personnes légitimes.

IV.5.3 Privacy by Design/by Default & DPIA

Privacy by Design/by Default

Des mesures techniques et organisationnelles appropriées sont mises en œuvre pour garantir, par défaut, que seules les données personnelles nécessaires au traitement sont traitées.

De telles mesures sont mises en œuvre dès la conception d'un traitement/produit/service, et offrent un niveau suffisant de protection des données permettant de respecter les droits des personnes concernées.

Ces mesures de sécurité et de protection des données personnelles sont intégrées au plus tôt dans la gestion des projets. Ces mesures doivent être adaptées et proportionnelles aux impacts sur la vie privée des personnes concernées évalués.

Une analyse d'impacts simplifiée est effectuée au préalable de la mise en place de traitements sur les données personnelles, pour identifier si le traitement est susceptible d'engendrer un risque élevé sur les droits et libertés fondamentales des personnes concernées et donc doit être soumis à une DPIA.

DPIA (ou Data Protection Impact Assessment)

Lorsqu'un traitement sur les données à caractère personnel est susceptible d'engendrer un risque sur les droits et libertés fondamentales des personnes concernées une analyse d'impacts sur la vie privée de ce traitement est réalisée. Les critères visant à déterminer la nécessité d'une analyse d'impacts sont ceux listées en préambule de la procédure analyse d'impacts

Cette analyse d'impacts est un processus ayant pour objectif de d'évaluer les impacts sur la vie privée des personnes concernées et de définir les mesures adéquates pour réduire les impacts.

Une méthodologie PIA a été définie et formalisée.

IV.6 Gestion des relations avec les tiers et/ou sous-traitants

Lorsque les activités de traitement sont déléguées à des tiers, le traitement **doit être régi par un contrat ou un autre acte juridique** comprenant au minimum les dispositions suivantes :

- Conformité aux exigences du GDPR
- Assistance, en particulier concernant les notifications de violations de données, les analyses d'impact, les formalités applicables et les demandes d'exercice des droits des personnes
- Respect de la sécurité et de la confidentialité des données
- Conditions d'appel à une sous-traitance ultérieure (Sidetrade doit au minimum pouvoir être informé et pouvoir s'y opposer)
- Conditions de contrôle par Sidetrade du respect des obligations du sous-traitant
- Conditions de restitution ou de suppression des données à l'issue de la prestation
- Description des actions attendues du prestataire dans le cadre de la prestation (instructions)

Le contrat légal ou un autre acte juridique doit stipuler que le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par le GDPR et de 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.

Le "tiers et/ou sous-traitants" des données doit informer le responsable du traitement des données si, à son avis, une instruction enfreint le présent règlement ou d'autres dispositions de l'Union ou des États membres en matière de protection des données.

Toute sous-traitance doit être en mesure de garantir et justifier des mesures de protection des données adéquates aux traitements effectués pour le compte du responsable de traitement. Ceci vaut aussi pour les traitements sur les données à caractère personnel où Sidetrade est « sous-traitant ». Sidetrade doit s'assurer que les sous-traitants proposent ce niveau adéquat de protection des données personnelles.

Lorsque Sidetrade fait appel à la sous-traitance, il est tenu de s'assurer que la personne concernée par le traitement sous-traité est informée et, selon les cas, a consenti à cette sous-traitance.

Le contrat légal ou un autre acte juridique doit que si le sous-traitant utilise les données à d'autres fins, les communique ou les utilise d'une manière non conforme aux termes du contrat, il sera considéré comme le responsable du traitement des données et **sera personnellement responsable des infractions** commises.

Le contrat légal ou un autre acte juridique doit que le "tiers et/ou sous-traitants" ne peut sous-traiter à un tiers un traitement qui lui a été commandé par le responsable du traitement, à moins d'avoir reçu l'autorisation de le faire.

IV.1 Gestion des transferts de données à caractère personnel (interne Sidetrade et hors UE)

Le transfert de données personnelles vers des pays en dehors de l'Union Européenne est interdit en règle générale. Pour qu'il puisse être autorisé, il doit nécessairement se conformer à certaines conditions, dont notamment :

- Le pays destinataire offre un niveau adéquat de protection des données selon la Commission Européenne, ou
- Les clauses contractuelles types de la Commission Européenne sont portées au contrat, ou
- La société destinatrice dispose de Règles d'Entreprise Contraignantes validées par la Commission Européenne, ou
- Dans le cas de transfert de données vers les Etats-Unis, la société destinataire a adhéré au « Privacy Shield »
- La personne concernée soit informée et consciente du transfert et que cela est conforme aux réglementations locales applicables. Les informations fournies aux personnes concernées concernant tout transfert de leurs données doivent inclure l'objet du transfert, l'identité du destinataire et les droits du sujet de données.

Les données personnelles ne peuvent être transférées à des tiers sans que la personne concernée soit **informée.** Dans certains cas, il sera nécessaire de demander le consentement de la personne concernée.

Le transfert des données personnelles en dehors de l'Union Européenne doit être autorisé par le DPO et la direction juridique après avoir obtenu l'assurance que cela est fait conformément à la présente politique et aux procédures applicables et aux exigences légales.

IV.2 Gestion des violations de données à caractère personnel

Sidetrade est tenu d'anticiper et de mettre en place les mesures nécessaires pour détecter et réagir en cas de violation des données personnelles.

En cas de violation, l'autorité de contrôle de la violation dans les 72h après avoir pris connaissance de la violation. Dans le cas où la violation est susceptible d'engendrer un risque élevé pour la personne concernée, une communication doit également être réalisée à destination de ces personnes.

Les modalités de gestion des violations de données à caractère personnel sont précisées dans la procédure éponyme.

IV.3 Formation/Sensibilisation

Il est important que tous les employés et les tiers de Sidetrade comprennent parfaitement leurs responsabilités dans le respect de toutes les politiques et procédures de protection des données personnelles. Les employés responsables de toute forme de traitement des données personnelles doivent être pleinement conscients de leurs obligations de ne pas collecter, traiter ou utiliser les

données personnelles sans autorisation appropriée, de maintenir les niveaux requis de confidentialité et de détecter et donner l'alerte en cas de violation de données.

Les employés de Sidetrade doivent s'engager à respecter la confidentialité lorsqu'ils prennent leurs responsabilités et avoir conscience que l'obligation de confidentialité continue après la fin de leur mission.

Les entités de Sidetrade sont tenues d'intégrer la formation sur la protection des données personnelles pour tous les employés à leurs besoins de formation existants afin de sensibiliser le personnel aux politiques et procédures connexes.

En outre, des sessions de formation/sensibilisation spécifiques doivent être organisées pour former les employés qui traiteront, non seulement des catégories particulières de données personnelles telles que les ressources humaines, mais aussi tous les métiers qui effectuent des traitements particuliers sur les données personnelles.