trusteam finance

PROCEDURE DE PROTECTION DES DONNEES A CARACTERE PERSONNELLE (GDPR)

Juin 2019

Sommaire

Rédacteur :		Approbateur :
Fabrice Pasqualini (RCCI)		Jean Luc Allain (Directeur Général)
REVISIONS		
Date	Nature de la modification	Version
18/05/2018	Rédaction initiale (CH)	V.1
18/06/2020	Mis à jour	V.2

1. SOURCES REGLEMENTAIRES

- Règlement 2016/679 du 27 avril 2016 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
- Directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

2. CONTEXTE

L'objectif de cette politique est d'expliquer les mesures prises par Trusteam Finance pour respecter ses obligations du règlement et de la directive sur la protection des données.

Le respect de cette politique est primordial pour que Trusteam Finance soit en capacité d'assurer une protection des données personnelles efficace en continu et de faire face aux incidents liés aux traitement et l'exploitation des données personnelles recueillis dans le cadre de son activité.

Le but de cette procédure est ainsi d'assurer meilleure gestion de ces données et d'accroître la confiance des partenaires.

3. FORMATION DES COLLABORATEURS ET DES DIRIGEANTS

Les collaborateurs et les dirigeants ont reçu une formation sur le règlement cité en référence. Cette formation fera l'objet d'actualisation en tant que de besoin (c'est-à-dire au fur et à mesure des développements de ce texte de référence et de son interprétation, notamment par la CNIL).

4. DEFINITIONS

Donnée à caractère Personnel : correspond à toute information permettant d'identifier directement ou indirectement une personne physique. Exemple : nom, adresse mail, numéro de téléphone, adresse postale…

Traitement intégrant des données à caractère personnel : correspond à tout process de collecte, d'utilisation, de conservation, transmission et maniement automatisé ou non qui s'applique à des données à caractère personnel. Exemple : collecte de données dans le cadre d'une ouverture de compte, envoi d'un reporting aux clients.

Responsable de traitement : désigne au sein de la société de gestion la personne en charge de recenser les différents traitements utilisant des Données à caractère Personnel et détermine les finalités de chacun de ces traitements (ci-après Responsable de traitement).

Sous-traitant et/ou prestataire : correspond à toute personne physique ou morale qui traite des Données à caractère Personnel uniquement sur instruction documentée du Responsable du traitement et pour le compte de ce dernier. Les sous-traitants et prestataires sont eux-mêmes soumis à une obligation de sécurité et de confidentialité des Données à caractère Personnel afin d'en assurer la protection et le correct traitement

5. TRAITEMENT DES DONNEES

5.1. Identification des traitements

Les traitements principaux sont de 4 natures :

- Les communications les informations de toute nature à destination des investisseurs,
- La connaissance par les gérants de la qualité de leurs clients afin de les servir au mieux de leurs intérêts,
- Les vérifications prévues dans le cadre d'une évaluation du « risque de blanchiment et de financement du terrorisme » (dispositif obligatoire)
- Le contrôle des risques « de passif » (ou « risques clients ») dans le cadre des tests de résistance aux rachats dans le cadre de la mesure de la liquidité des fonds.

Les données personnelles ne sont ni vendues ni transmises à des tiers.

5.2. Registre des traitements

La Société tient à jour un registre listant les traitements de données afin de recenser l'ensemble des traitements des données.

Ce registre a été complété par chacun des collaborateurs de Trusteam Finance.

Ce registre est divisé par typologie d'activité, en précisant :

- L'objectif poursuivi (la finalité – exemple : la fidélisation client)
- Les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire …)
- Qui a accès aux données (gestion collective, gestion privée, hébergeurs)
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est mis à jour à minima annuellement.

Les traitements purement occasionnels ne sont pas mentionnés dans le registre, conformément à la réglementation en vigueur.

Les collaborateurs de Trusteam veillent à ce qu'il n'y a pas de collecte d'information inutile.

5.3. Durée de conservation des données personnelles

La SGP conserve directement ou indirectement les données personnelles de ses clients jusqu'à 6 ans après la fin de leur relation, compte tenu des obligations législatives ou réglementaires qu'elle a l'obligation de respecter, et des pouvoirs d'enquête de l'AMF.

A l'issue des périodes de conservation légales ou réglementaires auxquelles est tenue la SGP, les données personnelles seront détruites selon les évaluations des risques de conservation de ces données et les protocoles de destruction qui auront été établis à ces fins sous la responsabilité des dirigeants.

5.4. Sécurisation de toutes les données collectées

Trusteam Finance met en place des mesures de sécurité physiques et organisationnelles sur son informatique afin de protéger les données personnelles stockées sur son serveur ou dans ses bases de données.

Les sous-traitants et prestataires sont eux-mêmes soumis à une obligation de sécurité et de confidentialité des Données à caractère Personnel afin d'en assurer la protection et le correct traitement.

5.5. Accessibilité des données personnelles aux autorités

Il est précisé que les personnes ayant autorité sur la SGP, notamment dans le cadre de la surveillance de ses activités soumises à leur agrément, sont habilités à prendre connaissance de l'ensemble des informations qui encadrent ces activités, y compris les données personnelles des clients et des partenaires dont la SGP dispose. Cette disposition relève d'une obligation légale.

6. VIOLATION DE LA CONFIDENTIALITE DES DONNEES

Une violation de données signifie que des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou un accès non autorisé à des données a été constaté.

Dans cette situation, la personne informée de cette violation doit obligatoirement la signaler au DPO sans délai si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées.

Si ces risques sont élevés pour ces personnes, la personne qui entretient la relation habituelle avec ces personnes devra les en informer.