trusteam finance

POLITIQUE PROTECTION DES DONNEES

Référence : RGPD
Création : 18/05/2018
Politique validée le : 22/05/2018 par Jean-Luc Allain.

Diffusion de la politique :

La politique est diffusée par la conformité par envoi par mail à tous les services/ collaborateurs concernés, puis par mise sur l'intranet accessible à l'ensemble des salariés de Trusteam Finance à l'emplacement dédié aux procédures, politiques et cartographies.

L'original signé est conservé par la conformité dans le classeur « Recueil de procédures et politiques de Trusteam Finance ».

Services / collaborateurs concernés : Tous les collaborateurs de Trusteam Finance

Sources réglementaires :

- 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

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, par conséquent, les salariés de Trusteam Finance ont bénéficié d'une formation spécifique. Les collaborateurs, bénéficiaires effectifs et dirigeants de Trusteam Finance doivent respecter cette politique.

A. Définition des concepts

Le règlement Général sur la Protection des Données (RGDP) vient renforcer la loi française de 1978 - Loi Informatique et Libertés.

Il est adopté le 27 avril 2016 par le Parlement Européen, et est entré en vigueur le 25 mai 2016. Il est applicable dès le 25 mai 2018.

Le champ d'application territorial du RGPD est défini selon trois notions clefs :
- Critère de l'établissement : Le règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
- Critère de ciblage : Le règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
- Dans le cadre de relation avec les représentants diplomatiques ou consulaires d'un état membre : Le règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

La protection conférée par le règlement s'applique aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. Ainsi, le critère de la nationalité n'est pas déterminant. En revanche sont pertinents : l'établissement du responsable du traitement ou du sous-traitant impliqué dans le traitement, ou le territoire dans lequel est fourni le bien ou le service.
Pour rappel, les clients ont :
- le droit à l'effacement
- le droit à la limitation
- le droit à la portabilité

L'encadrement du profilage présent dans les textes ne concerne pas Trusteam Finance.

Sont considérées comme donnée personnelle toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne peut être identifiée :
- Directement (nom, prénom)
- Indirectement (par un identifiant (n° client), n° de tél, un courriel, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, économique, culturelle ou sociale, la voix ou l'image).

L'identification d'une personne physique peut être réalisée :
- A partir d'une seule donnée (n° sécurité sociale, vaisseaux sanguins)
- A partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, ayant tel produit, et ayant telle adresse secondaire).

N'est pas considérée comme donnée personnelle un fichier ne contenant que des coordonnées d'entreprises.

Le traitement des données personnelles est une opération, ou un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé et les fichiers papier doivent donc être protégés dans les mêmes conditions.
A chaque traitement de données doit être assigné un but légal et légitime au regard de l'activité professionnelle.

Concernant les données RH, sont concernées les données liées au recrutement (la gestion des candidatures), la gestion du personnel (la formation, les évaluations, la rémunération, la protection sociale), l'utilisation des outils de l'entreprise par les salariés (connexion à une Interface). Les exemples donnés sont non-limitatives (pour avoir l'intégralité des finalités des traitements de données personnelles, se référer au fichier RGPD sur le réseau ou s'adresser au DPO en envoyant un courriel à dpo@trusteam.fr).

B. Descriptifs des enjeux et objectifs

Les enjeux du règlement RGPD se trouvent dans une meilleure maîtrise des données qui permettra une meilleure gestion du développement de l'entreprise et aussi une meilleure confiance des partenaires.

C. Les étapes suivies pour constituer le registre des traitements

1. Recensement des fichiers
2. Tri des données
3. Respect des droits des personnes
4. Sécurisation de toutes les données collectées

1. Le recensement des fichiers

La création d'un registre listant les traitements de données permet d'avoir une vision d'ensemble sur le traitement des données.
Les activités principales de Trusteam ont été définies selon les principaux services (gestion collective, gestion privée, développement commercial, recherche/analyse satisfaction client, fonctions support) nécessitant la collecte et le traitement de données (gestion des clients prospects, gestion de la paye, …).

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

Dans le registre, une fiche pour chaque activité recensée est créée, 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).

Ce registre exhaustif doit être mis à jour régulièrement.

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

2. *Le tri dans les données*

Pour chacune des fiches de registres créées, il a été vérifié par les collaborateurs :
- Que les données traitées sont nécessaires à chacune des activités de Trusteam Finance
- Qu'il n'y a aucun traitement de données dites « sensible », si c'est le cas, que Trusteam Finance a bien le droit de les traiter
- Que seules les personnes habilitées ont accès aux données dont elles ont besoin
- Que les données ne sont pas conservées au-delà de ce qui est nécessaire.

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

3. *Respect des droits des personnes*

Les personnes sont informées à chacune des collectes de données personnelles, le support utilisé comporte des mentions d'information. Les informations comportent les éléments suivants (texte suggéré entre guillemets à inclure dans les communications) :
- Pourquoi les données sont collectées (la finalité) : « Vos données personnelles sont collectées avec pour finalité la gestion ou le développement commercial ou l'analyse satisfaction client et le respect de la réglementation. »
- Ce qui autorise Trusteam Finance à traiter ces données (fondement juridique) « Trusteam Finance, de par son agrément en tant que société de gestion, est autorisée à les collecter et les traiter avec les finalités précédentes. »
- Qui a accès aux données : « Vos données peuvent être consultées par les collaborateurs de Trusteam. »
- Combien de temps les données sont conservées « Elles sont stockées pendant sept ans a minima à compter du début de la relation. »
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits « Vous pouvez exercer vos droits liés à la mise en application du Règlement Général de la Protection des données en envoyant un mail au DPO à dpo@trusteam.fr »
- La possibilité de transférer les données hors de l'Union Européenne. « Il vous est possible de demander le transfert des données hors de l'Union Européenne sur demande à votre interlocuteur habituel et en informant le DPO à dpo@trusteam.fr. »

Les personnes dont les données sont traitées ont des droits renforcés par le RGPD sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, de portabilité et de limitation du traitement. Cette information est intégrée dans les courriers adressés aux personnes concernées.

Dans le cadre de l'activité d'une société de gestion, la gestion privée et le développement sont impactés par le traitement à grande échelle de données à caractères personnelles. Toutefois, celles-ci ne sont pas sensibles et leur recueil est réglementairement obligatoire lors de l'entrée en relation.

Ainsi, Trusteam Finance a jugé que ce traitement ne constituait pas un traitement soumis à une obligation de consultation préalable de la CNIL. Il n'a donc pas été jugé nécessaire de réaliser une analyse d'impact (Privacy Impact Assessment, PIA).

4. Sécurisation de toutes les données collectées

Les mesures mises en œuvre pour assurer la sécurité des données sont le changement régulier des mots de passe, l'utilisation de mots de passe complexes et la gestion par un tiers des toutes les données.

D. Situation de breach

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.