Verband Schweizerischer Vermögensverwalter | VSV
Association Suisse des Gérants de Fortune | ASG
Associazione Svizzera di Gestori di Patrimoni | ASG
Swiss Association of Asset Managers | SAAM

Règlement européen sur la protection des données - conséquences pour les gestionnaires de fortune suisse

Chers Membres,

Que prévoit le règlement européen relatif à la protection des données ?

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (règlement général sur la protection des données, RGPD) entrera en vigueur le 25 mai 2018. Le règlement est directement applicable dans l'ensemble de l'Espace économique européen/EEE (c'est-à-dire les États membres de l'UE, l'Islande, le Liechtenstein et la Norvège), sans qu'aucune transposition ne soit nécessaire dans les divers États. L'objectif du règlement est de donner aux citoyens un plus grand contrôle sur leurs données personnelles, de sensibiliser les entreprises sur leurs responsabilités et de renforcer le rôle des autorités chargées de la protection des données.

Le **champ d'application matériel** du RGPD couvre le traitement entièrement ou partiellement automatisé des données à caractère personnel qui sont stockées dans un système de fichiers ou qui doivent être stockées. Toutes les informations relatives à une personne physique sont considérées comme des données personnelles. Le RGPD ne couvre pas les données des personnes morales.

Le c**hamp d'application territorial** a été étendu par rapport à l'ancienne directive sur la protection des données (directive 95/46/CE). Le critère du groupe cible de personnes concernées par le traitement des données figure désormais au premier plan. Le règlement s'applique donc également aux entreprises ayant un établissement dans l'Union européenne, dans la mesure où le traitement des données à caractère personnel a lieu dans le cadre des activités dudit établissement (**Notion d'établissement**). En outre, les entreprises établies dans des pays tiers, comme la Suisse, qui offrent des biens ou des services à des personnes dans l'EEE ou qui observent le comportement de personnes physiques dans l'EEE par le biais de leur traitement de données peuvent être concernées (**principe des effets**). Ceci peut alors entraîner une application extraterritoriale du RGPD pour les entreprises en Suisse.

Que signifie le RGPD pour les gérants de fortune suisses entretenant des relations professionnelles avec des clients résidant dans l'EEE ?

La question de savoir si un gérant de fortune suisse doit se conformer au RGPD dépend en premier lieu du fait s'il propose ou non des services à des personnes physiques dans l'EEE. Le RGPD ne prévoit aucune définition exacte du terme de l'offre des biens et services. La littérature professionnelle contient des déclarations controversées à ce sujet.

Le **considérant 23 du RGPD** précise qu'il doit être établi «s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union». A cet égard, les sites web provenant du pays tiers concerné accessibles aux résidents de l'EEE dans une langue qui leur est familière, l'utilisation d'adresses électroniques couramment utilisées dans ce pays ou d'autres données de contact, ne constituent pas encore des indices suffisants selon lesquelles l'offre est faite à des personnes dans un ou plusieurs états de l'EEE. En revanche, les références sur des sites web à des investissements qui s'adressent à des personnes dans certains États de l'EEE ou particulièrement adaptés à ces personnes sont naturellement à considérer comme des indications claires qu'une offre est faite à des personnes dans ces États. En matière de protection des consommateurs, les autorités de l'UE se sont basées dans le passé sur «l'impression générale» de la communication d'entreprise, comme l'utilisation de "Top-Level-Domains" orientés sur des activités étrangères ou internationales (*.eu, mais également *.com), sans pour autant déterminer si de tels indices sont à eux seuls décisifs. S'adresser directement à des personnes dans l'EEE par le biais de courriers, messages électroniques et autres formes de contacts directs est, en revanche, un indice manifeste et difficilement réfutables d'une offre.

Dans ce contexte, il faut également rappeler que selon le principe de la libre prestation de services passive, le gérant de fortune suisse ne peut fournir de service, sans l'agrément de l'EEE correspondant, que sur la seule initiative du client, conformément à l'art. Art. 42 de MiFID II (RL 2014/65/UE). En dépit de formulation différente des dispositions applicables (MiFID II et RGPD), il ne serait pas cohérent, du point de vue de l'ASG, d'interdire la fourniture de services d'investissement, mais de qualifier parallèlement la fourniture de services sur l'initiative du client comme une «offre» au sens de la RGPD. Il faudra néanmoins probablement des années avant que ces questions ne soient finalement clarifiées. Néanmoins, il est déjà largement reconnu dans la doctrine que la fourniture de services à des clients finaux dans l'EEE (en particulier sur leur propre initiative) ne fonde à elle seule l'application du RGPD.

Pour évaluer si un gérant de fortune suisse est soumis ou non au RGPD, il convient toutefois toujours d'examiner sa situation particulière. C'est la **vue d'ensemble** de la situation qui démontre s'il y a une intention manifeste de proposer des marchandises et services au sein de l'EEE.

Si un gérant de fortune suisse estime que le RGPD s'applique à ses activités, il doit répondre à plusieurs **obligations**.

Tout d'abord, il doit déterminer quelles données sont collectées et traitées, pour quelles finalités, où, quand, comment et par qui. Une documentation des processus internes est indispensable. Un inventaire des données ainsi traitées doit être dressé. Le traitement des données relatives aux personnes en dehors de l'EEE ne relève pas du RGPD.

Dans le sens **d'une approche fondée sur les risques, les mesures nécessaires** doivent alors être prises. Celles-ci peuvent, par exemple (liste non exhaustives) consister en :

- la mise en œuvre des obligations d'information à l'égard des personnes dont les données sont traitées (par exemple au moyen d'une déclaration de confidentialité qui divulgue aux personnes concernées la nature et l'étendue des données traitées);
- des adaptations ou compléments aux contrats de gestion de fortune existants (déclarations de consentement - privilégier la forme écrite pour des raisons de preuve - du client dont les données font l'objet d'un traitement);
- la mise en place de processus internes pour garantir les droits des personnes concernées. (Droit d'information, de divulgation, de rectification, de suppression et d'opposition);
- des mesures organisationnelles et techniques de protection (en particulier, la désignation d'une personne responsable du Compliance dans le domaine de la protection des données).

Enfin, nous attirons votre attention sur le fait qu'en septembre 2017, le Conseil fédéral a soumis aux Chambres le message sur la **révision totale de la loi fédérale sur la protection des données (LPD)**. L'objectif de ce projet est de moderniser la LPD et de l'aligner sur la législation européenne en matière de protection des données afin de maintenir un niveau de protection comparable à celui de l'UE et de conserver ainsi la déclaration d'adéquation existante de l'UE.

Nous nous tenons volontiers à votre disposition pour toute question ou complément d'information.

Meilleures salutations

Association Suisse des Gérants de Fortune | ASG