Zurich, aout 2023

Les gestionnaires de fortune et la loi révisée sur la protection des données – Des effets limités en raison d'un traitement des données prévu par la loi

(Un guide pour les praticiens du secteur des services financiers rédigé par Alexander Rabian, Melanie Käser et Mathias Stauffacher, avocats, Streichenberg und Partner[1])

Traitement de données sur la base d'une obligation légale

Alors que dans le cadre de la précédente LPD, le traitement des données à caractère personnel était une justification générale du traitement des données à caractère personnel en raison d'une obligation légale (art. 27, al. 1 ancienne LPD), la loi révisée sur la protection des données (LPD) du 1er septembre 2023, nécessite une approche plus différenciée à certains égards.

Les principales exigences légales pour les gestionnaires de fortune en matière de traitement des données des clients figurent dans les lois suivantes sur la surveillance des marchés financiers (conformément à l'art. 3, al. 1, Loi sur la surveillance des marchés financiers, LFINMA):

- Loi du 15 juin 2018 sur les services financiers (LSFin)
- Loi du 10 octobre 1997 sur la lutte contre le blanchiment d'argent (LBA)
- Loi du 15 juin 2018 sur les établissements financiers (LEFin)
- Loi du 23.6.2006 sur les placements collectifs de capitaux (LPCC)
- Loi du 19 juin 2015 sur l'infrastructure des marchés financiers (LIMF)

Pour toutes ces lois fédérales au sens formel, il existe des ordonnances d'exécution (du Conseil fédéral, en partie aussi de l'Autorité fédérale de surveillance des marchés financiers FINMA), qui fournissent également une base légale pour le traitement des données personnelles.

Parmi les lois susmentionnées, la LBA et la LSFin ont les exigences les plus étendues pour le traitement des données personnelles concernant les « clients » au sens large, c'est-à-dire les parties contractantes et les personnes qui leur sont

[1] Traduction libre de l'ASG. Pour le texte original, cf. Lien

Streichenberg und Partner
Stockerstrasse 38
8002 Zürich
Schweiz
T. +41 44 208 2525
www.streichenberg.ch

liées (par exemple, les bénéficiaires économiques / détenteurs de contrôle, les représentants et autres personnes liées ou commercialement/personnellement liées).

Le traitement des données à caractère personnel concernant les employés de sa propre entreprise est également soumis à des conditions découlant du droit des marchés financiers (par exemple les garants de l'activité irréprochable), du droit du travail ou du droit des assurances sociales.

Réglementation fondée sur les risques

Le droit suisse de la surveillance des marchés financiers se caractérise, entre autres, par le fait qu'il prévoit une « approche fondée sur les risques » pour de nombreux domaines réglementaires. Ce principe de base doit également être pris en compte pour déterminer quelles données personnelles doivent être traitées par un conseiller / gestionnaire de fortune en raison d'une exigence légale.

La loi (p. ex. la LBA et ses dispositions d'exécution telles que l'OBA-FINMA) ne détermine pas de manière concluante quelles données à caractère personnel doivent/peuvent être traitées dans le cadre d'une réglementation fondée sur les risques. La loi consacre des principes (tels que le principe du « KYC ») et stipule que l'institution financière réglementée doit prendre toutes les précautions nécessaires (y compris le traitement des données personnelles) pour s'assurer que des états de fait reconnus par la loi comme illicites ou indésirables ne se matérialisent pas. L'établissement financier réglementé doit identifier, recenser et gérer systématiquement les risques de comportements illicites ou indésirables générés par ses activités commerciales (autorisées), c'est-à-dire mener une véritable gestion des risques.

En raison des lois rédigées de manière abstraite, il n'est donc pas possible de déterminer de manière univoque quelles données personnelles des clients, des partenaires contractuels, des employés et des prestataires de services doivent être traitées par un établissement financier réglementé ou un intermédiaire financier réglementé afin de se conformer à ses obligations légales. À cet égard, les lois ne prescrivent pas de « valeurs maximales » des données personnelles à traiter, mais fixent – le cas échéant – des normes réglementaires minimales.

En raison de la réglementation basée sur les risques, chaque prestataire de services financiers doit déterminer lui-même, entre autres, quelles données personnelles il souhaite traiter afin de se conformer aux exigences légales. Il dispose d'un pouvoir discrétionnaire considérable pour ce faire.

Les gestionnaires de fortune autorisés par la FINMA doivent disposer d'un vaste ensemble de directives, qui doivent être approuvées par leurs autorités de surveillance (FINMA et organismes de surveillance) et qui sont périodiquement contrôlées par les auditeurs chargés de s'assurer qu'ils sont correctement organisés pour répondre aux exigences légales. Ce n'est pas le dépassement des exigences légales en matière d'identification, de mesure et de gestion des risques qui est examiné, mais plutôt la non-conformité aux exigences minimales. Le système de directives

doit également avoir pour objet un système de contrôle interne (SCI) proportionné à l'étendue et à la complexité des opérations commerciales ainsi qu'aux risques pour les investisseurs et, en particulier, pour l'intégrité et la réputation de la place financière. La gestion d'un tel SCI nécessite également le traitement de données personnelles sur les clients, les organes, les employés, mais aussi sur les employés occupant des fonctions clés chez les partenaires d'externalisation et même chez les fournisseurs.

Le gestionnaire de fortune, ses organes de direction, employés et auxiliaires externes doivent toujours être garants d'une activité irréprochable et jouir d'une bonne réputation. Les personnes impliquées dans l'entreprise ne doivent pas avoir d'influence négative sur la garantie d'activité irréprochable. Cette exigence de garantie implique le traitement de données personnelles concernant les employés dans une mesure qui dépasse le cadre des entreprises sans exigence de garantie légale correspondante. Le cadre exact doit être déterminé par le gestionnaire de fortune en application de l'approche basée sur les risques. En outre, les données personnelles concernant les employés en charge des clients doivent établir qu'ils ont les connaissances juridiques et l'expertise suffisantes.

Même en cas d'utilisation de données à caractère personnel collectées en exécution d'obligations légales et traitées à des fins de marketing, le traitement des données correspondant par les conseillers et les gestionnaires de fortune peut se fonder sur les exigences légales. Dans le contexte de l'offre de produits financiers, la LSFin stipule en effet que les données à caractère personnel des investisseurs potentiels et effectifs seront traitées dans le cadre de la classification de la clientèle à effectuer (y compris tout opting-in ou opting-out), du respect des obligations d'information et du respect des exigences relatives à l'offre d'instruments financiers.

En résumé, on peut dire que la réglementation des services financiers fondée sur les risques accorde aux institutions financières et aux intermédiaires financiers une grande autonomie pour déterminer quelles données personnelles doivent ou devraient être traitées. L'approche réglementaire fondée sur les risques prescrit également le traitement de données à caractère personnel particulièrement sensibles (à l'exception peut-être de données de santé très spécifiques) et prévoit également le traitement de profils de personnalité (en particulier de clients, d'employés, de personnes clés chez des partenaires externalisés) avec des données à caractère personnel particulièrement sensibles (par exemple, des informations sur les activités politiques dans le cadre des règles relatives aux relations avec les personnes politiquement exposées).

Applicabilité des principes de base de la nouvelle LPD (ci-après LPD)

Les principes juridiques de base suivants en matière de protection des données s'appliquent également si le responsable du traitement dispose d'une justification légale pour le traitement des données :

- Principe de légalité (art. 6 al. 1 LPD): dans le cas d'un gestionnaire de fortune agréé, il est rempli par des bases juridiques étendues ainsi que par des intérêts privés ou publics supérieurs dans un cadre large ;

- Principe d'opportunité (art. 6 al. 1 LPD): Les données ne peuvent être utilisées, sans respect des autres dispositions de la LPD, qu'à des fins légales. Cependant, celles-ci vont très loin ;
- Principe de proportionnalité (art. 6 al. 2 LPD): Les données ne peuvent être traitées que dans la mesure nécessaire à la finalité prévue. La réglementation basée sur les risques définit ici un cadre général et donne au gestionnaire sa propre discrétion ;
- Bonne foi (art. 6 al. 2 LPD) : Le respect des exigences légales est toujours un traitement de données de bonne foi. Ce principe limite le traitement des données à l'application appropriée d'une approche fondée sur les risques, mais laisse au responsable du traitement une large marge d'appréciation ;
- Obligation de transparence/obligation d'information (art. 6 al. 3 LPD / art. 19 et suivants LPD) : les données traitées sont obtenues dans un but reconnaissable. Cette exigence est satisfaite simplement en informant les clients, les investisseurs, etc. ;
- Paramètres par défaut respectueux de la vie privée (art. 7 LPD ; « Privacy by Design/Default ») : Ce principe est relativisé dans une très large mesure par les lois de surveillance applicables. Souvent, les paramètres par défaut respectueux de la vie privée sont en contradiction avec les buts et objectifs de la réglementation ;
- Exactitude des données (art. 6 al. 5 LPD) : Les lois de surveillance applicables stipulent que le gestionnaire de fortune doit être convaincu de l'exactitude des données personnelles traitées. Le traitement intentionnel ou négligent de données à caractère personnel affecte l'obligation de garantir une activité irréprochable. Certaines lois sur la surveillance des marchés financiers prévoient une vérification fondée sur les risques de l'actualité et de l'exactitude des données à caractère personnel traitées ;
- Sécurité des données (art. 8 LPD): les directives doivent inclure des exigences appropriées en matière de sécurité des données.

Registre des activités de traitement (art. 12 LPD)

Les activités de traitement de données à caractère personnel effectuées par un gestionnaire de fortune découlent de ses directives. Un registre des activités de traitement des données doit être établi, sauf si l'entreprise emploie moins de 250 personnes et si des données à caractère personnel particulièrement sensibles ne sont pas traitées ou si un profilage à haut risque est effectué.

Néanmoins, étant donné que les gestionnaires de fortune traitent régulièrement des données à caractère personnel particulièrement sensibles dans le cadre de leurs obligations légales, en particulier en vertu de la LBA, et peuvent même effectuer un profilage à haut risque, il est conseillé en l'état des connaissances actuelles de tenir un registre des activités de traitement des données

Il n'est pas nécessaire de conserver des listes détaillées de chaque élément de données traitées (« listes avec champs de données ») lorsque les données à caractère personnel sont traitées électroniquement dans le cadre des directives. Précisément lors de la mise en œuvre d'une approche fondée sur les risques du trai-

tement des données à caractère personnel à des fins réglementaires, des caractéristiques de données identiques ne sont pas traitées schématiquement pour tous les clients, bénéficiaires économiques ou représentants. En outre, le registre des activités de traitement ne doit pas nécessairement être un document distinct du système de directives, mais peut y être intégré.

Communication de données à l'étranger (art. 16 et suivants LPD)

La communication de données à l'étranger n'est pas interdite en soi. Cela signifie que les gestionnaires de fortune peuvent continuer à traiter les données sur des serveurs et des installations de stockage de données à l'étranger.

L'annexe I de Ordonnance sur la protection des données (OPDo) énumère les États et territoires qui, selon le Conseil fédéral, disposent d'un niveau adéquat de protection des données. Outre les États de l'EEE, de nombreux autres pays sont également reconnus comme ayant un niveau adéquat de protection des données. Mais pas les États-Unis. Le traitement des données sur des serveurs situés aux États-Unis n'est donc autorisé que dans une mesure limitée.

Devoir d'informer lors de la collecte de données personnelles (art. 19 et suivants LPD)

La transparence du traitement des données comprend également l'obligation d'informer de manière adéquate la personne concernée sur le traitement des données à caractère personnel. t. L'article 19 LPD prévoit l'obligation d'informer lors de la collecte de données. Dans le cadre de leurs obligations légales (en particulier en vertu de la LBA), les gestionnaires de fortune obtiennent non seulement des informations sur les clients (etc.) desdits clients, mais utilisent également d'autres sources de données (par exemple pour vérifier la plausibilité des données collectées auprès du client). Il va sans dire que les données que le gestionnaire de fortune reçoit directement du client sont traitées.

Selon l'art. 20 LPD, l'obligation de fournir des informations sur l'acquisition de données ne s'applique pas dans la mesure où le traitement correspondant des données est prévu par la loi. Cela s'applique en particulier au traitement des données des clients et des données personnelles concernant les employés. En ce qui concerne les clients, l'obligation d'information est largement supprimée en raison du secret professionnel. Même si les données à caractère personnel sont communiquées à l'étranger en conformité avec l'art. 16 LPD (par exemple stockées sur un serveur), les personnes concernées ne doivent pas en être spécifiquement informées.

Une déclaration de protection des données complète et détaillée vis-à-vis des clients et des employés n'est donc pas nécessaire pour les gestionnaires de fortune qui déploient une activité dite classique. Toutefois, il est néanmoins logique, dans le cadre des exigences générales de transparence, d'informer les clients sur le

traitement étendu des données prévu par la loi dans le cadre des obligations générales d'information. Il est important que le gestionnaire de fortune indique dans ces informations que son entreprise est responsable du traitement des données.

Toutefois, le gestionnaire de fortune qui traite des données à caractère personnel dans un contexte plus large, telles que les données à caractère personnel des candidats à un emploi, est légalement tenue d'informer ces personnes du type, de l'étendue et de la durée du traitement des données.

Les gestionnaires de fortune ayant un modèle d'affaire fortement ou partiellement basé sur la communication et la fourniture de services en ligne ont également des obligations d'information plus larges. L'intégration d'applications Web dans la gestion de fortune nécessite le traitement de données personnelles (par exemple, des enregistrements électroniques de l'utilisation de l'application Web), qui ne sont pas couverts par des exigences légales, mais résultent du modèle commercial spécifique et des accords contractuels correspondants. Ces gestionnaires de fortune traitent les données à caractère personnel dans un cadre qui va au-delà des exigences légales et ont des obligations d'information plus étendues, ce qui rend nécessaire une déclaration complète de protection des données.

Les dispositions relatives à l'utilisation de « cookies » sur les sites Internet restent inchangées. L'obligation d'information reste en vigueur. La nouvelle loi sur la protection des données ne prévoit pas d'obligation de consentement.

Traitement des données pour le compte des banques

Dans le cadre de la délégation d'obligations formelles au titre de la LBA, les gestionnaires de fortune traitent régulièrement des données à caractère personnel aussi pour le compte des banques « délégantes » (« délégation » en vertu de la CDB). Cela implique pour le gestionnaire de fortune le traitement des données personnelles pour le compte du tiers qui constitue en même temps son propre traitement de données requis par la loi.

Étant donné qu'il s'agit d'un traitement concomitant de données à caractère personnel, que le gestionnaire de fortune doit également traiter lui-même conformément aux exigences légales, aucune précaution particulière n'est nécessaire pour le gestionnaire de fortune pour le traitement de ces données.

Si le gestionnaire de fortune traite des données à caractère personnel et les transmet aux banques dépositaires, ce qui est normalement le cas pour la « délégation » des obligations formelles de diligence raisonnable en vertu de la CDB, mais également pour le traitement ultérieur des données (par exemple, la préparation du KYC), le client concerné doit en être informé. Cela peut être généralement fait dans le cadre de l'information générale des clients.

Communication de données à des tiers, en particulier à des sous-traitants

Si le gestionnaire de fortune fait traiter des données à caractère personnel par des tiers en Suisse ou à l'étranger, il veille dans les contrats correspondants à ce que

le traitement des données par le sous-traitant ne soit effectué que d'une manière conforme aux règles applicables au gestionnaire de fortune. À cette fin, les contrats devraient contenir des clauses appropriées en matière de protection des données.

En particulier, le gestionnaire de fortune doit également s'assurer, au moyen de clauses appropriées, que le sous-traitant a pris les précautions nécessaires pour protéger le secret professionnel. Les exigences réglementaires de la FINMA en matière d'externalisation s'appliquent.

Devoir d'informer en cas de décision individuelle automatisée (art. 21 LPD)

Les classifications de risques selon la LBA ou en ce qui concerne les activités d'investissement selon la LSFin (classification sur la base de questionnaires) ne constituent pas des « décision individuelle automatisée » au sens de la LPD, même si des systèmes informatiques fournissent des résultats. En raison des exigences réglementaires, il incombe personnellement aux personnes responsables de prendre les décisions appropriées. Les « automatismes » utilisés ne sont que des aides.

Analyse d'impact relative à la protection des données (art. 22 LPD)

Cette obligation ne s'applique pas si le traitement des données est effectué en vertu d'une obligation légale (art 22 al. 4 LPD).

Annonce des violations de la sécurité des données (art. 24 LPD) ; Procédure selon la Communication FINMA

Les gestionnaires de fortune exercent une activité supervisée. Les exigences légales en matière de traitement des violations de la sécurité des données en vertu de la LPD sont donc en partie largement dépassées par les exigences de l'autorité de surveillance, la FINMA. En particulier dans le cas de cyberattaques contre des fonctions dites « critiques » (qui comprennent également les systèmes informatiques), les exigences de la communication de surveillance de la FINMA 05/2020 doivent être respectées. Le principal organe à informer est l'OS. La FINMA doit également être mise au courant en cas de procédure d'autorisation en cours.

Seules les atteintes internes à la sécurité des données (par exemple l'accès aux données des clients par des employés non autorisés) doivent être signalées au Préposé fédéral (PFPDT) si elles peuvent présenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Dans la pratique, cependant, ce risque élevé n'existe que s'il existe une menace de « fuite de données vers l'extérieur ». Dans de tels cas, cependant, l'autorité de contrôle responsable doit être informée de toute façon. Les informations fournies au PFPDT doivent être coordonnées avec l'autorité de surveillance.

Les principes de procédure doivent être fixés dans les directives.

Droit d'accès (art. 25 et suivants LPD)

Il s'agit en particulier de la relation entre le droit à l'information de la loi sur la protection des données et les obligations d'information et de reddition de la LSFin. En raison du secret professionnel inscrit dans la LEFin, les données à caractère personnel ne peuvent pas être divulguées à des personnes autres que le maître du secret concerné, sauf s'il existe des obligations légales particulières de divulgation. Les lois sur la surveillance prévoient également d'autres motifs de refuser, de restreindre ou de différer (art. 26, al. 2 LDP) la communication des renseignements. Cela inclut des informations sur le respect de l'obligation de communiquer en vertu de la LBA et d'autres obligations réglementaires de communiquer, les obligations de confidentialité dictées par des autorités et le « no tipping off » en vertu du droit national et étranger (par exemple en matière fiscale).

Compte tenu de ces nombreuses restrictions possibles au droit à l'information, il y a de bonnes raisons pour considérer que la LSFin définit le cadre d'information pour le conseil et la gestion de fortune. Dans le cas des activités d'intermédiaire financier au sens de la LBA, le refus, la restriction ou le simple retard dans la fourniture d'informations est une conséquence du caractère procédural pénal préventif de la LBA. Le droit à l'information ne doit pas être utilisé pour mettre en péril les objectifs de la LBA (prévention et lutte contre le blanchiment d'argent et le financement du terrorisme). En cas de doute, le gestionnaire de fortune autorisé doit restreindre ou même refuser de fournir des informations prévues par la LPD. Cela doit être décidé au cas par cas.

Restrictions

Les explications ci-dessus ne s'appliquent que dans une mesure limitée si

A. les données relatives aux personnes physiques sont collectées à des fins autres que la fourniture de services de gestion de fortune, de conseils en investissement, la réception et la transmission d'ordres portant sur des instruments financiers et l'offre d'instruments financiers (par exemple dans le cadre d'une inscription en ligne à une newsletter destinée à des non-clients);

B. le traitement des données ne relève pas seulement du champ d'application de la LPD, mais également du champ d'application des lois sur la protection des données de l'Union européenne, en particulier du RGPD. À cet égard, il convient toutefois de noter que, dans le présent avis, l'acceptation et la gestion des clients résidant dans l'EEE dans le cadre de la libre prestation passive des services (considérants 111, phrase 2, MiFID II et 43, phrase 2, MiFIR) n'entraînent pas l'application du RGPD.

***