Jacqueline Sievers

Dr en droit, LL. M., avocate, CIPP/E
Walder Wyss AG, Zurich
www.walderwyss.com

David Vasella

Dr en droit, avocat, CIPP/E
Walder Wyss AG, Zurich
www.walderwyss.com

Droit de la protection des données

Signification du RGPD pour la branche fiduciaire

En Europe, le droit de la protection des données est adapté à l'évolution des conditions-cadres. Le règlement général sur la protection des données (RGPD), qui a aussi des conséquences sur les entreprises suisses, est entré en vigueur dans l'UE et l'EEE le 25 mai 2018 et le 1er juillet 2018. Dans cet article, les auteurs examinent l'applicabilité du RGPD aux fiduciaires et à leurs clients en Suisse et présentent les obligations et les exigences organisationnelles qui en résultent.

Tous ceux qui traitent des données personnelles devaient déjà depuis longtemps[1] respecter toute une série de principes de la protection des données, notamment les suivants:[2]

- licéité (art. 4 al. 1 LPD)
- traitement conforme aux principes de la bonne foi (art. 4 al. 2 LPD)
- proportionnalité (art. 4 al. 2 LPD)
- caractère reconnaissable et but (art. 4 al. 3 et 4 LPD)
- exactitude des données (art. 5 LPD)
- sécurité des données (art. 7 LPD)
- limitation de la communication des données personnelles à l'étranger (art. 6 LPD)

La protection des données n'a donc nullement besoin d'être réinventée. Ce n'est cependant un secret pour personne que la protection des données connaît ou connaissait un certain déficit en termes d'exécution,[3] en Suisse tout comme dans le reste de l'Europe.

Le règlement général européen sur la protection des données (RGPD)[4] prévoit par conséquent des sanctions qui doivent être «effectives, proportionnées et dissuasives» (art. 83 al. 1 RGPD), et accompagne les **obligations matérielles** des sous-traitants de données d'**obligations de documentation et d'organisation complémentaires** (art. 5 al. 2 RGPD, «Responsabilité»; mais aussi de dispositions sur le délégué à la protection des données, le représentant dans l'UE, l'évaluation des conséquences en matière de protection des données, la gestion des manquements à la protection des données personnelles, l'implication des sous-traitants, etc.). La Suisse vise une législation analogue au RGPD et révise actuellement sa législation sur la protection des données (LPD).[5] Même si le **projet de LPD** (P-LPD) en est encore au stade de la consultation,[6] on peut supposer que la nouvelle LPD ressemblera au RGPD, bien qu'avec des nuances et – c'est à espérer – avec une approche beaucoup plus pragmatique.[7]

Le débat se focalise cependant toujours sur le RGPD, qui est entré en vigueur le 25 mai 2018 dans l'UE et le 20 juillet 2018 dans le reste de l'EEE[8]: il s'agit en l'occurrence principalement de l'**application extra-territoriale** du RGPD[9] et des craintes ainsi provoquées – et nourries par le secteur du conseil –, principalement à propos des amendes élevées (qui sont toutefois exagérées pour les entreprises sans succursale dans l'EEE), des avertissements formulés par l'Allemagne (sachant que seuls quelques avertissements pour manquements au RGPD sont connus et qu'il n'a pas encore été établi s'ils pouvaient tout simplement donner lieu à des avertissements)[10] et de la charge bureaucratique requise par la mise en œuvre du RGPD. Dans ce contexte, on peut se demander dans un premier temps si et quand le RGPD sera applicable aux fiduciaires en Suisse et à leurs clients.

1. Le RGPD est-il applicable aux fiduciaires suisses et à leurs clients?

1.1 Généralités

Il ne fait aucun doute que les fiduciaires relèvent du champ d'application matériel du RGPD. Ils traitent des informations se rapportant à des personnes physiques identifiées ou identifiables et donc des données personnelles (art. 4 nº 1 et 2 RGPD). Il en va de même de leurs clients.

La question de savoir dans quelles circonstances le champ d'application géographique du RGPD est ouvert est, en revanche, moins claire. Nous devons distinguer deux cas de figure à cet égard:

- Si **un tribunal ou une autorité** dans l'EEE se penche sur cette question, l'art. 3 RGPD qui règle l'applicabilité territoriale du RGPD est applicable (cf. à ce sujet les points 1.2 ss.). Les dispositions en matière de conflit de lois du droit local dans l'État du tribunal qui déterminent le champ d'application territorial du droit de transposition (c.-à-d. qui décident par exemple quel droit matériel national règle les limitations des droits et devoirs des art. 12 ss. RGPD sur la base de l'art. 23 RGPD).[11]
- Si un **tribunal suisse ou une autorité suisse** doit statuer sur l'application du RGPD, ce n'est en revanche pas l'art. 3 RGPD qui est applicable, mais le droit suisse des conflits de loi; autrement dit l'art. 139 LDIP dans le cas de prétentions déduites d'un prétendu manquement au droit

de la protection des données.[12] Une invocation directe de l'art. 3 pour justifier l'applicabilité du RGPD devant un tribunal suisse est donc exclue (même si les auteurs disposent d'une première action qui entend fonder les prétentions directement sur l'art. 3 RGPD).

L'attention se porte néanmoins sur l'art. 3 RGPD, parce que les risques d'une amende sont jugés plus élevés que les risques de prétentions civiles devant des tribunaux suisses. L'art. 3 RGPD règle trois cas dans lesquels le RGPD s'applique à un traitement de données par une personne ou une entreprise en dehors de l'EEE. D'importantes incertitudes subsistent encore pour tous ces cas. Une certaine clarification est attendue du **Comité européen de protection des données**, une commission des autorités de surveillance des États membres (l'ancien Groupe de travail «Article 29» sur la protection des données) qui a notamment pour mission de rechercher l'application uniforme du RGPD (art. 67 ss. RGPD). Nous savons que ce comité a adopté le 25 septembre 2018 des orientations générales sur l'art. 3 RGPD en vue d'une consultation publique, mais celles-ci n'avaient pas encore été publiées à la date d'impression de cet article.

1.2 Succursale dans l'EEE

Si une entreprise détient une succursale dans l'EEE, le RGPD est applicable aux traitements de données «en relation» avec cette succursale (art. 3 al. 1 RGPD). De nombreuses questions sont en suspens, p.ex. quelle relation entre une succursale et l'entreprise suisse suffit pour que le RGPD soit également applicable à cette dernière et ce qu'est d'ailleurs une «succursale» dans le sens de la protection des données. En la matière, la constatation selon laquelle les entreprises suisses ayant **des filiales, des succursales et d'autres structures durables dans un État de l'EEE** courent au moins le risque de devoir respecter le RGPD également pour leurs propres activités.

1.3 Offre de marchandises ou de prestations

Le RGPD ne peut toutefois pas restreindre son applicabilité aux entreprises domiciliées dans l'EEE. Afin de protéger les personnes concernées dans l'EEE, il doit aussi couvrir les traitements des données en dehors de l'EEE. Dans ce contexte, l'art. 3 al. 2 let. a RGPD ancre également le principe du lieu où se tient le marché connu dans d'autres domaines juridiques.[13] Ainsi, le RGPD s'applique à des traitements de données «en relation» avec des «offres» à des personnes concernées dans l'Union (c.-à-d. l'EEE). Si une entreprise fiduciaire adresse une offre à des personnes dans l'EEE, le RGPD peut être applicable aux offres correspondantes.

Est qualifiée d'«offre» toute **offre de prestations** payante ou gratuite, que l'offre soit suivie de la conclusion d'un contrat ou non.[14] Le texte ne couvrant de toute évidence que les offres et non la demande de prestations, le traitement de données en relation avec le recrutement, l'engagement et l'emploi de personnes à l'étranger (p.ex. des frontaliers) ne devrait pas relever du RGPD.[15] Sont donc couvertes les offres à des personnes qui séjournent physiquement dans l'EEE; le domicile et la nationalité importent peu, tout comme le séjour habituel (cf. considérant 2). À l'inverse, les offres **qui s'adressent à des personnes morales ne sont pas couvertes**, car seules des personnes physiques sont des personnes concernées dans le sens du RGPD (art. 4 nº 1 RGPD). L'offre d'une représentation pour la TVA en Suisse pour une entreprise étrangère ne relève par exemple pas de l'art. 3 al. 2 let. a RGPD. Il importe cependant peu de savoir si la personne physique contactée agit en qualité de consommateur ou à titre professionnel, les affaires B2B pouvant donc également être couvertes. Une entreprise fiduciaire qui propose des prestations à des entreprises individuelles peut donc parfaitement relever du RGPD.

La restriction suivante est toutefois très importante: l'art. 3 al. 2 let. a RGPD ne couvre que les offres qui s'adressent **de toute évidence à des personnes physiques dans l'EEE** (considérant 23; «de toute évidence envisagé»). Il faudra déterminer au cas par cas à l'aide de critères objectifs si c'est le cas. Le considérant 23 cite quelques indices et d'autres résultent de la jurisprudence applicable de la Cour de justice européenne.[16] La conception du site Internet devrait notamment être importante pour les fiduciaires sans succursale dans l'EEE. Les indices suivants suggèrent notamment une intention évidente:

- Utilisation d'un domaine d'un État de l'EEE, tel que «.de» ou «.fr»
- Utilisation d'une langue parlée dans l'EEE qui n'est pas une langue nationale suisse, p.ex. polonais
- Description de prestations spécifiques pour des personnes de l'EEE (p.ex. offres de conseil pour l'imposition des frontaliers Suisse-France ou informations sur des offres de conseils pour des particuliers conjointement avec un partenaire allemand)
- Indication de prix en EUR ou dans une autre monnaie européenne
- Description du trajet depuis le pays étranger dans l'EEE jusqu'en Suisse
- Évocation de la clientèle dans l'EEE, p.ex. dans des témoignages
- Dépenses, p.ex. pour Google AdWords, pour que le site Internet soit trouvé à l'étranger.

Les clients aléatoires de l'EEE qui sont certes servis, mais sans qu'une intention correspondante n'ait été manifestée ne sont donc pas couverts, sauf si l'on considère déjà la conclusion du contrat comme un indice suffisant pour une telle intention, ce que nous ne jugeons toutefois pas justifié.[17]

La situation n'a pas été clarifiée en ce qui concerne les **relations durables qui n'ont pas été activement prospectées**, par exemple une relation avec un client allemand qui a été acquis sur le territoire de la Suisse, mais qui vit en Allemagne et continue d'être suivi, même après son retour au pays. On peut se demander comment doivent être traitées les offres supplémentaires dans le cadre de ce suivi, par exemple en cas de prolongation ou de développement de la relation client. Nous pensons que les offres dans le cadre d'une telle relation existante ne devraient pas être en mesure de déclencher l'applicabilité du RGPD. De telles offres se situent dans le cadre d'une relation client existante et ne déploient donc pas l'effet de dispersion dont il est question à l'art. 3 al. 2 let. a RGPD selon le considérant 23.

Le traitement des **offres internationales générales**, par exemple sur un site Internet en anglais sous un nom de domaine .com. L'exploitant du site Internet peut faire valoir que son offre a certes un caractère international, mais qu'elle ne s'adresse pas, du moins pas de façon «évidente», à des personnes dans l'EEE. Cet argument est particulièrement important pour les prestataires américains qui relevaient toujours du RGPD; mais ne serait-ce que pour des raisons d'égalité de traitement, il devrait également être admis pour des exploitants suisses.

Au final, la situation juridique manque de clarté à de très nombreux égards. Il est donc judicieux d'examiner le propre site Internet afin de déterminer s'il comporte des indices d'une focalisation sur des clients privés dans l'EEE et de les poursuivre sciemment (avec les conséquences correspondantes) ou d'adapter le site Internet en conséquence.

1.4 «Suivi du comportement»

Le RGPD est par ailleurs applicable au suivi du «comportement» des personnes concernées, pour autant que le comportement soit suivi dans l'EEE (art. 3 al. 2 let. b RGPD). Comme le montre le considérant 24, le législateur s'intéresse ici au **tracking en ligne** et aux activités comparables. On considère alors comme «suivi», le traitement conscient de données personnelles qui renseignent sur le comportement de personnes physiques qui se trouvent dans l'EEE pendant le suivi du comportement (le domicile et la nationalité étant de nouveau sans importance). Seul est toutefois couvert le suivi personnel, ce qui soulève la question de savoir quelles informations sont considérées comme des données personnelles dans le domaine en ligne. Bien que cette question ne soit pas clarifiée en ce qui concerne les

adresses IP et les informations similaires,[18] on peut estimer que les tribunaux et les autorités de surveillance traiteront ces données comme des données personnelles, sans faire vraiment de distinction.[19] Au final, l'exigence de la référence à une personne ne restreint donc guère l'applicabilité spatiale du RGPD dans le domaine du suivi du comportement.[20]

Il importe donc peu de savoir si le suivi concerne sciemment des personnes dans l'EEE.[21] Il est en revanche nécessaire que le suivi soit pratique avec une certaine **intensité et durée**.[22] Cela ne ressort pas uniquement de la compréhension habituelle de la notion de «suivi», mais se déduit également du considérant 24. Nous pensons qu'une entreprise fiduciaire ne devrait pas relever de l'art. 3 al. 2 let. b RGPD au seul motif qu'elle utilise un logiciel tel que Google Analytics pour mesurer le volume des visiteurs. On pourrait par ailleurs se demander si un suivi éventuel du comportement dans cet exemple serait vraiment imputable à l'entreprise qui ordonne le suivi du comportement en impliquant Google Analytics, ou seulement à Google en sa qualité d'entreprise qui effectue le suivi du comportement.[23]

Là encore, il subsiste donc de nombreuses incertitudes. Une autre s'y ajoute: le suivi des activités sur Internet relève-t-il du suivi du comportement ou aussi du suivi du **comportement qui se déroule hors ligne**? Cela peut par exemple être important en cas de recours, dans le cadre d'un mandat de gestion de fortune, aux comptes d'une personne physique, des recettes et des dépenses occasionnées dans l'EEE étant alors suivies. La littérature tend à refuser une application dans le domaine hors ligne, en raison de la restriction au considérant 24, mais ce point n'a pas non plus encore été clarifié.[24]

Au final, le RGPD peut notamment s'appliquer aux sites Internet, dès lors que des technologies qui enregistrent le comportement des visiteurs sont utilisées, du moins si une certaine intensité est atteinte de ce fait dans le cas concret. Il existe ici un risque (plutôt minime à ce jour) d'une réprimande, notamment en provenance d'Allemagne, par exemple si le site Internet ne dispose pas d'une déclaration de confidentialité conforme au RGPD.[25]

1.5 Autres cas

En dehors des cas de figure cités (succursale; orientation de l'offre, suivi du comportement), le RGPD ne requiert pas d'application. C'est également le cas si une entreprise domiciliée en Suisse confie le traitement de données personnelles à un sous-traitant sur le territoire de l'EEE, p.ex. à un hébergeur allemand. Dans ce cas, le sous-traitant est certes assujetti au RGPD, raison pour laquelle il présentera un contrat conforme au RGPD; le mandant suisse n'est toutefois pas assujetti au RGPD de ce fait.[26]

Nous pensons que les situations suivantes n'entraînent **pas** en elle-même **l'application du RGPD**:[27]

- le traitement de données personnelles en relation avec une offre à des clients entreprises ou avec l'activité pour ces derniers, même si l'offre s'adresse expressément à des entreprises suisses (p.ex. dans le cas des représentations pour la TVA)
- le traitement de données personnelles en relation avec un mandat d'une personne physique qui a été obtenu sans focalisation sur le marché étranger et ce même si le mandat a été renouvelé ou réédité au cours de la relation.
- l'entretien d'une liste d'adresses de clients entreprises, même si des données personnelles (p.ex. indication d'interlocuteurs) sont traitées à cette occasion
- l'externalisation d'activités de traitement à un sous-traitant (p.ex. un prestataire informatique) dans l'EEE
- l'emploi de collaborateurs étrangers en Suisse

Le RGPD peut en revanche être applicable à des prétentions de droit civil, lorsqu'un tribunal suisse doit appliquer un droit étranger, aux termes de l'art. 139 LDIP. Ce serait notamment le cas si une personne qui séjourne habituellement dans un État de l'EEE formule des **prétentions à l'endroit d'un sous-traitant suisse** et invoque le droit de son pays à ce titre. Dans ce cas, on pourrait envisager qu'un tribunal suisse accorde un dédommagement immatériel (art. 82 al. 1 RGPD); mais une amende ne serait pas envisagée.

2. Principales obligations des fiduciaires concernés selon le RGPD

Si le RGPD est applicable à une certaine activité de traitement, il doit être respecté pour ladite activité.[28] Les principales exigences du RGPD sont par conséquent esquissées ci-après.

2.1 Obligations de documentation

Comme indiqué en introduction, le RGPD ne se fie pas à des obligations matérielles. La documentation du respect de la protection des données (art. 5 al. 2 RGPD; «Responsabilité») et, partant, la tenue d'un **registre des procédures** (art. 30 RGPD) constitue peut-être l'obligation parallèle la plus importante. S'agissant du premier point, la tenue d'un journal, d'un registre central des processus pertinents en droit de la protection des données (p.ex. des demandes des personnes concernées avec date de réception et de règlement; des évaluations des conséquences de la protection juridique ou de la renonciation à une telle, etc.) est recommandée, au moins dans les PME.[29] Le deuxième point, le registre des procédures, est réglé à l'art. 30 RGPD. Ainsi les responsables tout comme les sous-traitants doivent tenir des registres de leurs traitements de données (pour autant qu'ils relèvent du RGPD). Le registre ne saisit pas chaque traitement de données (c.-à-d. pas chaque client individuellement), mais certaines catégories de traitements de données (p.ex. la gestion des données de clients). L'art. 30 al. 1 et 2 RGPD prescrit la teneur minimale des registres et des modèles ainsi que des exemples sont disponibles sur Internet.[30] Le projet de LPD révisée prévoit également une obligation de tenir un registre des activités de traitement (art. 11 P-LPD).

L'obligation de procéder à une **évaluation des conséquences de la protection des données** (une sorte de «contrôle de compatibilité avec la protection des données») et de la déclarer, le cas échéant, à l'autorité de surveillance compétente (art. 35 et 36 RGPD; là encore, il existe une correspondance dans le projet de LPD, art. 20) s'apparente aux obligations de documentation. Le RGPD n'indique que de façon marginale quand il y a vraisemblablement des risques élevés (art. 35 al. 3 RGPD). Les autorités de surveillance ont cependant publié des listes selon l'art. 35 al. 4 RGPD et à ce sujet. Une obligation d'évaluation des conséquences ne devrait pas être fréquente dans le cas des entreprises fiduciaires. Une telle obligation est cependant envisageable dans les grandes entreprises fiduciaires, qui gèrent principalement des particuliers et dans les «analyses Big Data» des données de clients qui ont été enrichies d'informations émanant de sources tierces.[31]

2.2 Exigences organisationnelles

Les entreprises dont les activités de traitement relèvent du RGPD mais qui ne disposent pas d'une succursale dans l'EEE (art. 3 al. 2 let. a et b RGPD) sont tenues de désigner un représentant dans l'EEE (art. 27 RGPD). Le **représentant dans l'UE** fait office d'interlocuteur pour les autorités de surveillance et les personnes concernées et tient donc lieu de boîte aux lettres se substituant à la succursale manquante. Il doit en outre tenir une copie des registres de procédure (art. 30 al. 1 et 2 RGPD) pour que les autorités puissent se faire une idée des activités de traitement correspondantes sans passer par l'entraide administrative. La désignation s'effectue au moyen d'un mandat idoine et le représentant dans l'UE doit être cité dans les déclarations de protection des données (art. 13 et 14 RGPD, respectivement al. 1 let. a). Une exception à l'obligation de nomination s'applique cependant quand le traitement correspondant (c.-à-d. relevant du RGPD) n'est qu'occasionnel, ne concerne aucune catégorie particulière de données personnelles et n'entraîne pas de risques déterminants pour les personnes concernées (art. 27 al. 2 RGPD). Les entreprises fiduciaires

petites et moyennes pourront pour le moins invoquer régulièrement cette situation exceptionnelle, en tous cas lorsque la gestion de clients privés étrangers ne représente qu'une petite partie de l'activité.

Le RGPD exige ensuite la nomination d'un **délégué à la protection des données** (interne ou externe) (art. 37 RGPD). Une telle obligation n'est cependant effective que si l'«activité de base» de l'entreprise consiste en une surveillance complète, régulière et systématique ou en un traitement complet de données personnelles particulières, ce qui n'est généralement pas le cas des entreprises fiduciaires. La désignation d'une personne responsable de la protection des données est néanmoins utile. Elle ne devrait cependant pas être qualifiée de «délégué à la protection des données», de «Data Protection Officer», etc., pour éviter toute confusion avec la fonction du délégué à la protection des données officiel dans le sens de l'art. 37 RGPD.[32]

2.3 Déclarations de protection des données et CG

Selon la LPD en vigueur, les personnes concernées ne doivent être préalablement informées du traitement de leurs données personnelles que s'il ne semble pas évident (art. 4 al. 3 LPD: «qui découle des circonstances ou qui est prévu par la loi») ou que des données personnelles sensibles ou des profils de la personnalité sont collectés (art. 14 LPD). À défaut, les personnes concernées ont besoin du registre public de certains fichiers (art. 11a LPD) et surtout du droit d'accès (art. 8 LPD). À l'instar de la LPD révisée (art. 17ss. P-LPD), le RGPD suit une toute autre approche: une **information complète et active** sur chaque traitement de données (art. 12ss. RGPD) doit être communiquée par avance, même à propos des traitements évidents. Seules quelques exceptions sont prévues à cette règle.[33] Les fiduciaires doivent par conséquent informer activement les clients, les collaborateurs et les partenaires sur les traitements qui relèvent du RGPD. Le devoir d'information inclut notamment les données de contact de l'entreprise, les finalités et bases juridiques du traitement (à savoir p.ex. l'exécution du mandat, la gestion des données de clients, le marketing, etc.), les catégories de données personnelles traitées, la durée d'enregistrement des données, les destinat aires éventuels des données personnelles en Suisse et à l'étranger et les droits des personnes concernées. Afin de répondre à ce devoir d'information, l'entreprise responsable devra publier une déclaration ou des déclarations de protection des données, p.ex. sur un site Internet, le cas échéant aussi en complétant les conditions générales. Une obligation correspondante mais de moindre ampleur résultera également de la LPD révisée.

Selon le RGPD, les données personnelles ne doivent par ailleurs être traitées que si une **autorisation** correspondante est effective; à défaut le traitement est interdit (art. 5 al. 1 let. a, art. 6 et art. 9 RGPD).[34] Le traitement de données personnelles pour des mandats s'appuie avant tout sur la base juridique de la préparation et de l'exécution du contrat (art. 6 al. 1 let. b RGPD). Dans la mesure où des catégories particulières de données personnelles dans le sens de l'art. 9 al. 1 RGPD sont également traitées à cette occasion, p.ex. des données concernant la santé, une autre base juridique est cependant requise. Un **consentement** exprès sera requis en la matière, qui peut cependant être généralement demandé par le biais des CG (expressément acceptées).[35] La conception d'une déclaration de consentement juridiquement sûre constitue cependant une tâche exigeante. Dans la plupart des cas, des consentements sont également requis pour l'envoi d'une publicité électronique; mais toutefois moins en raison du RGPD que selon l'art. 3 al. 1 let. o LCD ou (lors de l'envoi à des personnes à l'étranger) selon le droit local applicable en matière de comportement sur le marché,[36] jusqu'à ce que celui-ci soit remplacé dans l'UE et l'EEE par l'ordonnance e-privacy. – Les consentements peuvent être révoqués en tout temps (p.ex. le consentement à recevoir une newsletter). Les activités de traitement pour lesquelles il existe un consentement et celles pour lesquelles il a été révoqué doivent donc être documentées.[37]

2.4 Respect des droits des personnes concernées

Étant donné que le droit de la protection des données entend assurer le pouvoir de détermination des personnes concernées sur leurs données personnelles, les personnes concernées ont certains droits en relation avec le traitement de leurs données (droits dits des personnes concernées). Ces droits peuvent être catégorisés en droits visant à assurer la transparence (les droits à l'information, à une copie des données personnelles et aux informations complémentaires selon l'art. 15 RGPD et à être entendu dans les décisions individuelles automatisées qui ne seront pas approfondies ici), à assurer l'intégrité des données (le droit de rectifier et de compléter selon l'art. 16), à limiter le traitement des données (les droits à l'effacement selon l'art. 17, à la limitation du traitement selon l'art. 18 et à l'opposition selon l'art. 21) et le droit à la portabilité des données (art. 20).

Ce n'est pas nouveau en principe; la LPD accorde également une série de droits de la personne concernée (p.ex. le droit d'accès selon l'art. 8 LPD; mais désormais moins complets que le RGPD). La gestion des droits des personnes concernées selon le RGPD est néanmoins exigeante. D'une part, la teneur des droits des personnes concernées n'est pas toujours claire et bon nombre de détails sont contestés. D'autre part des questions liées au processus sont également ouvertes, p.ex. l'**identification correcte** des personnes concernées. En principe, les demandes doivent néanmoins être traitées dans un délai de **trente jours** (art. 12 al. 3 RGPD). Au moins dans le cas de grandes entreprises, il est donc conseillé de prévoir ou d'adapter des processus internes correspondants. Le nombre de demandes n'a cependant pas connu d'augmentation sensible à ce jour.

2.5 Effacement de données

Tout comme la LPD en vigueur, le RGPD exige que les données personnelles soient effacées si elles ne sont plus requises et s'il n'y a pas d'obligation de conservation. La mise en œuvre de cette obligation n'est cependant pas une tâche facile. Dans un premier temps, une entreprise doit se faire une idée des données personnelles traitées et des flux de données correspondant et les registres de procédures peuvent s'avérer utiles à cet égard. Une durée de conservation qui se déduit p.ex. des obligations de conservation légales doit ensuite être attribuée à chaque catégorie de données personnelles. Pour finir, et c'est la partie la plus exigeante, il faut s'assurer grâce à des mesures techniques et à des instructions aux collaborateurs que les délais de conservation sont si possible respectés et que les données des systèmes productifs sont archivées à temps.[38]

2.6 Externalisations des traitements de données

L'externalisation des traitements de données est fréquente et ne pose aucun problème en principe. Le RGPD privilégie l'externalisation par rapport aux communications à d'autres tiers, aucune base juridique particulière n'étant requise. L'externalisation est par conséquent autorisée s'il s'agit également du traitement externalisé, sous réserve d'interdictions légales ou contractuelles d'externaliser. Ce privilège est toutefois conditionné par la **conclusion d'une convention avec le sous-traitant** qui le soumet au contrôle par le responsable. L'art. 28 al. 3 RGPD prescrit par conséquent les teneurs minimales d'une telle convention.[39] Dans la mesure où une entreprise fiduciaire relève du RGPD et externalise des traitements importants (relevant du RGPD) à un sous-traitant en Suisse ou à l'étranger, elle est tenue de conclure une convention correspondante.[40] À l'inverse, les sous-traitants ayant une succursale dans l'EEE sont tenus de conclure une telle convention, raison pour laquelle les prestataires d'envergure ont souvent déjà adapté leurs CG.

Si le sous-traitant se trouve à l'étranger, les exigences à l'égard de la **transmission de données personnelles à l'étranger** doivent en outre être respectées. Si un niveau de protection des données approprié fait défaut dans le pays de destination, ce qui est par exemple le cas des États-Unis, de l'Inde et de la Chine, la transmission n'est souvent autorisée qu'après la conclusion d'un contrat de transmission des données suffisant.[41] Lors des transmissions aux États-Unis, il est en outre possible que le destinataire se soit soumis au Privacy Shield, un programme visant à assurer une protection appropriée des données. Dans ce cas, il existe un niveau de protection suffisant pour le destinataire concerné pour les transmissions couvertes par la certification.[42]

2.7 Sécurité des données

Tout comme selon la LPD suisse, les données personnelles doivent également être suffisamment protégées contre les risques, notamment l'accès illicite, la perte et la destruction, selon le RGPD (art. 5 al. 1 let. f, art. 24 et 32 RGPD). Des mesures appropriées d'ordre technique et organisationnel doivent être prises à cet effet (p.ex. en restreignant l'accès aux données ou aux locaux, p.ex. au moyen d'un système de badges, du cryptage des ordinateurs portables, d'instructions, etc.). L'obligation de signaler à l'autorité de surveillance compétente les manquements à la protection des données dans un délai de 72 heures et d'en informer éventuellement aussi la personne concernée (art. 33s. RGPD; «Breach Notification») vise également la sécurité des données. Le droit suisse de la protection des données en vigueur ne connaît pas une telle obligation à ce jour, du moins pas de façon expresse. La LPD révisée prévoira cependant une Breach Notification (art. 22 P-LPD).

3. Conclusions

À l'instar de la plupart des entreprises, les entreprises fiduciaires en Suisse doivent se demander si elles doivent ou veulent concrétiser le RGPD. Cette question s'inscrit cependant dans le contexte de la révision de la LPD, car de nombreuses exigences du RGPD se retrouveront également dans la LPD révisée. Dans ce contexte, une mise en œuvre du RGPD sert également de préparation à la LPD révisée. De nombreuses entreprises dont l'activité se concentre sur la Suisse, mais qui ne peuvent néanmoins pas exclure une application du RGPD ont donc opté pour une mise en œuvre modérée: le RGPD sert de fil directeur à la compliance en matière de protection des données, mais sans que l'entreprise renvoie expressément au RGPD et la mise en œuvre suit une approche pragmatique (requise lors de chaque mise en œuvre du RGPD) et renonce à une pression inutile. Cette forme de mise en œuvre mesurée a fait ses preuves selon les auteurs.

Au final, une procédure telle qu'énoncée ci-après devrait convenir à de nombreuses entreprises fiduciaires – sachant qu'elle n'est ni définitive, qu'elle ne doit pas nécessairement suivre cet ordre et qu'elle peut aussi être parallèle:

- Désignation d'une personne responsable de la protection des données; si nécessaire s'assurer d'un soutien externe
- Saisie des données personnelles traitées dans l'entreprise et des processus de traitement des données (registres de procédures)
- Vérification de la présence en ligne du point de vue technique et des contenus
- Le cas échéant, désignation d'un représentant dans l'UE
- Élaboration des déclarations de protection des données et vérification et, le cas échéant, adaptation des CG et des documents contractuels
- Vérification des contrats avec les prestataires
- Vérification des procédures internes, par exemple dans les domaines du personnel, du marketing et de l'étendue avec les données de mandats.
- Vérification de la durée de conservation des données personnelles et le cas échéant lancement de l'élaboration d'un concept d'effacement ■

1 La loi fédérale sur la protection des données est entrée en vigueur le 1er juillet 1993.

2 Selon la présentation, cette liste pourrait être complétée par l'interdiction de la transmission de données personnelles particulières à des tiers (art. 12 al. 2 let. c LPD) et de la liberté de traitement des données personnelles publiées (art. 12 al. 3 LPD).

3 Cf. à ce sujet le rapport du Conseil fédéral du 9 novembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255 («[…] il est rare que les personnes lésées engagent une procédure judiciaire, […] L'application des nouvelles technologies ne fait pour sa part quasi jamais l'objet d'une procédure judiciaire»).

4 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; il a remplacé la Directive relative à la protection des données (Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données).

5 La révision ne vise pas uniquement le rapprochement avec le RGPD, mais aussi la mise en œuvre de la Convention remaniée du Conseil de l'Europe nº 108; cf. à ce sujet le message du 15 septembre 2017, FF 2017, 6586ss. À propos de la révision, cf. p.ex. David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, Jusletter du 27 novembre 2017; Jacqueline Sievers/David Vasella, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, 44ss.

6 Le Conseil national en débattra durant la session hivernal 2018 en tant que premier conseil.

7 Actuellement, il n'est par exemple pas prévu d'introduire en Suisse un droit à la portabilité des données, tel qu'il est inscrit à l'art. 20 RGPD. Nous pensons qu'il faudrait renoncer à un tel droit.

8 L'espace économie européen (EEE) inclut l'UE, ses États membres et la Principauté de Liechtenstein, ainsi que l'Islande et la Norvège.

9 Cette expression est utilisée ici, parce qu'elle est devenue courante; dans les faits il s'agit cependant moins d'extra-territorialité que des conditions dans lesquelles un traitement de données peut être qualifié d'intra-territorial.

10 Il existe des jugements allemands contradictoires à cet égard.

11 Les lois d'application contiennent généralement leurs propres dispositions en matière de droit des conflits d'intérêts, même si elles pourraient laisser cette question aux règles préexistantes en matière de droit des conflits d'intérêts; cf. par exemple le § 1 al. 4 de la loi allemande sur la protection des données (BDSG) (aux termes de laquelle la BDSG peut déjà s'appliquer quand un traitement de données a lieu en Allemagne; cette approche est également suivie par la LPD liechtensteinoise qui n'a pas encore été adoptée) ou l'art. 5-1 al. 1 de la Loi française nº 78-17 relative à l'informatique, aux fichiers et aux libertés (aux termes de laquelle le droit d'application français relatif à la protection des personnes concernées et de la souveraineté nationale s'applique toujours lorsque la personne concernée est domiciliée en France). Cf. à propos de l'ensemble aussi les réflexions formulées dans l'Étude d'impact française – Projet de Loi relatif à la protection des données personnelles, 12 décembre 2017, 71 ss.

12 Cf. à ce sujet l'arrêt du Tribunal administratif fédéral A-7040/2009 du 30 mars 2011, en la cause Google Streetview, consid. 5 (jugé en dernière instance dans l'ATF 138 II 346 par le Tribunal fédéral). Le principe de territorialité s'applique dans le domaine du droit public; vous trouverez également des informations à ce sujet dans l'arrêt cité du Tribunal administratif fédéral.

13 À ce propos Klar, in: Kühling/Buchner (éd.), Datenschutz-Grundverordnung/BDSG, 2e éd. 2018, Art. 3 N 6 ss.

14 Piltz, in: Gola (éd.), DS-GVO, 2e éd. 2018, Art. 3 N 28.

15 Des exceptions sont envisageables, par exemple en ce qui concerne l'offre de prestations de «relocation».

16 Par exemple dans l'arrêt de la CJCE du 7 décembre 2010 – Alpenhof, Cm C 585/08 et C 144/09, Cm 81 et 83.

17 A. A. Plath, in: Plath (éd.), DSGVO – BDSG, 3e éd. 2018, Art. 3 DSGVO N 23 (la conclusion du contrat suffit).

18 À ce propos Kühling/Buchner-Klar, Art. 4 Nr. 1 N 25 ss.

19 À ce sujet, ils vont invoquer le texte de l'art. 4, nº 1 RGPD, même s'il ne prescrit pas clairement cette conclusion: «[…] est réputée être une ‹personne physique identifiable› une personne physique qui peut être identifiée, […], notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou […]».

20 Les fournisseurs de logiciels de «tracking» exigent d'ailleurs plus fréquemment que leur client attire l'attention sur l'utilisation du logiciel dans sa déclaration de protection des données.

21 Kühling/Buchner-Klar, Art. 3 N 101.

22 Kühling/Buchner-Klar, Art. 3 N 94 s.; Zerdick, in: Ehmann/Selmayr (éd.), DS-GVO, 2e éd. 2018, Art. 3 N 20.

23 Si le responsable et pas (uniquement) le sous-traitant était toujours soumis au RGPD dans une telle configuration, l'art. 3 al. 2 RGPD («par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union») aurait dû être formulé différemment.

24 Ainsi Kühling/Buchner-Klar, Art. 3 N 92; Plath-Plath, Art. 3 DSGVO N 27; sans doute aussi Ennöckl, in: Sydow (éd.), Europäische Datenschutzgrundverordnung, 2e éd. 2018, Art. 3 N 15; Ernst, in: Paal/Pauly (éd.), DS-GVO BDSG, 2e éd. 2018, Art. 3 N 19; a priori aussi Meyerdierks, in: Moos/Schefzig/Arning (éd.), Die neue Datenschutz-Grundverordnung, 2018, p. 50; avis divergent de Lewinski, in: Auernhammer (éd),DSGVO BDSG, 5e éd. 2018, Art. 3 N 18; sans réponse: Gola-Piltz, Art. 3 N 31.

25 Cf. à ce sujet ci-dessus.

26 Näher Vasella, Zum Anwendungsbereich der DSGVO, digma 2017, 220 ss.

27 Il n'est toutefois pas exclu que le droit d'un État membre s'applique dans de tels cas; cf. note de bas de page 11.

28 Dans les entreprises de l'EEE, l'applicabilité est donc toujours ponctuelle, c.-à-d. limitée à une seule activité de traitement soumise au RGPD.

29 Il ne faut pas oublier qu'un tel journal doit être remis aux autorisés à leur demande, d'autres questions se posant en cas de demandes d'autorités étrangères (p.ex. en référence à l'art. 271 CP).

30 Cf. p.ex. http://datenrecht.ch/liechtenstein-muster-eines-verarbeitungsverzeichnisses.

31 En référence à la liste correspondante de la Conférence allemande en matière de protection des données, www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

32 En cas de ressemblance trop forte des désignations, on pourrait partir du principe d'une désignation volontaire d'un délégué à la protection des données, dans le sens de l'art. 37 RGPD; cf. à ce sujet les «Guidelines on Data Protection Officers» (rev.01) du Comité européen de la protection des données du 5 avril 2017.

33 Sur la base de l'art. 23 RGPD, les États membres peuvent prévoir d'autres situations exceptionnelles, ce que l'Allemagne a p.ex. fait aux § 32 s. BDSG. La Suisse ne peut en revanche pas prévoir de situations exceptionnelles, puisqu'elle n'est pas un État membre.

34 La LPD en vigueur mais aussi révisée poursuivent au contraire une autre approche: en conformité avec le droit général de la personnalité, un traitement des données est en principe recevable, pour autant qu'il comprenne des principes de traitement. La question d'une justification ne se pose qu'en cas de manquement aux principes. 35 En règle générale, l'assentiment à un traitement des données n'est certes pas jugé volontaire, s'il devient une condition, raison pour laquelle il ne peut pas être demandé dans les CG («interdiction de couplage»; cf. l'art. 7 al. 4 RGPD et le considérant 43). Si l'exécution d'un contrat n'est toutefois pas possible sans le traitement de données personnelles particulières, mais qu'aucune autre justification dans le sens de l'art. 9 al. 2 RGPD ne prévale, l'assentiment est objectivement nécessaire, de sorte que l'interdiction de couplage ne s'applique pas dans ce sens.

36 En Allemagne, le § 7 al. 2 ch. 3 et al. 3 de la LCD allemande exige en principe l'assentiment à l'envoi de publicité électronique.

37 Dans la mesure où il s'agit de l'assentiment au marketing, il ne suffit guère dans ce cas de rayer simplement un destinataire qui s'y oppose de la liste d'expédition, d'autant plus s'il y a un risque pour que son adresse soit de nouveau ajoutée subrepticement à une liste d'expédition.

38 Cela peut être déterminé dans un concept dit d'effacement. Pour le développement de concepts d'effacement, il existe des normes spécifiques, par exemple la norme ISO 66398.

39 La LPD renonce à prescrire des contenus minimaux, de même la LPD révisée.

40 Chaque prestataire n'est cependant pas un sous-traitant. Le champ d'application de la sous-traitance est souvent surévalué. La FAQ de l'Office de la surveillance de la protection des données du Land de Bavière est utile à cet égard (www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf): il n'y a sous-traitance que si une entreprise «est principalement chargée de traiter des données à caractère personnel», un traitement des données parallèle ou accessoire par le prestataire ne suffit pas. Ne sont par exemple pas des sous-traitants dans leur domaine typique les banques, les opérateurs de téléphonie, les services postaux et d'expédition, les cabinets d'avocats, les services de placement, les instituts de nettoyage, les prestataires de services d'impression, etc.

41 Cf. les art. 46 et 49 RGPD; les clauses contractuelles standard de l'UE sont généralement utilisées dans la pratique. La transmission fondée sur un consentement exprès est également recevable, ce qui n'est praticable que de façon exceptionnelle dans la réalité; la transmission en vue de la conclusion ou de l'exécution d'un contrat avec la personne concernée ou avec un tiers dans l'intérêt de la personne concernée (art. 49 al. 1 let. b et c RGPD) est plus importante.

42 Le Privacy Shield est toutefois mis sous pression par la Commission européenne. Pour plus de sûreté, il est donc conseillé de conclure un contrat de transmission de données également avec les entreprises certifiées.