FIDUCIAIRE|SUISSE Union Suisse des Fiduciaires

PROTECTION DES DONNÉES DANS LA BRANCHE FIDUCIAIRE

un guide de FIDUCIAIRE|SUISSE

version 1 - juillet 2018

FIDUCIAIRE | SUISSE

LA PROTECTION DES DONNÉES NOUS CONCERNE TOUS

Depuis le 25 mai 2018, après une période de transition de deux ans, le règlement général de l'UE sur la protection des données (RGPD) est applicable dans tous les pays de l'Union Européenne (UE) et de l'Espace Économique Européen (EEE). Sur la base du principe dit de marché le RGPD est également applicable directement aux entreprises en dehors de l'UE dans le cas où elles traitent des données de personnes de l'UE (ou de l'EEE) et si le traitement de ces données sert à proposer des biens ou des services à des personnes de l'UE ou de l'UEE ou à observer le comportement de personnes de l'UE ou de l'UEE

Mais pas toutes les affaires transfrontalières mènent automatiquement à l'applicabilité de RGPD. Il est néanmoins judicieux d'examiner de telles situations de manières approfondie. De plus dans la pratique, les entreprises de l'UE exigent souvent de manière explicite le respect par contrat du RGPD et des explications correspondantes.

Le RGPD a attiré l'attention du grand public sur le thème de la protection des données. Pourtant les principes généraux de la protection et du traitement des données sont restés identiques pour l'essentiel. Selon le RGPD et la loi fédérale sur la protection des données (LPD) les données ne peuvent être traitées que si cela est fait de manière légale. En particulier, il faut lors du traitement des données tenir compte des principes de la bonne foi, de proportionnalité et de finalité. Le RGPD n'y change rien. Cependant de nombreuses questions demeurent encore inexpliquées dans votre domaine. Il sera possible de répondre à ces questions au cours du temps.

La protection est un thème central pour la branche fiduciaire, pas uniquement pour des raisons juridiques mais aussi entrepreneuriales. C'est pourquoi FIDUCIAIRE|SUISSE met ce guide à la disposition de ces membres afin qu'ils puissent approfondir le thème de la protection des données et ainsi mettre leur entreprise et leurs clients «en condition» sur la protection des données en général et en particulier sur le RGPD. Ce guide vise à fournir des informations générales et n'est pas définitif. Il n'évite pas de se confronter avec le sujet et si nécessaire de faire appel à des tiers. Le guide vise à sensibiliser le thème de la protection des données et d'identifier des solutions potentielles dans le domaine de la branche fiduciaire.

La première partie (FAQ protection des données et RGPD) répond à des questions générales. La deuxième partie (protection des données dans la branche fiduciaire) se penche sur les thèmes importants pour la branche fiduciaire, site internet / newsletter / réseaux sociaux / personnel et clientèle. Pour finir, des check-lists avec des exemples d'activités fiduciaires typiques qui évaluent de manière générale si le RGPD est applicable ou pas, si le traitement des données a lieu légalement et qui expliquent les principaux éléments à prendre en compte.

Actuellement la loi fédérale sur la protection des données est en révision. Il faut s'attendre à de nombreuses adaptations au RGPD. C'est pourquoi il est important que même les fiduciaires qui n'entrent pas dans le champs d'application de la règlementation de l'UE se penchent sur le thème. De plus, les clients et les partenaires exigent fréquemment des explications.

FAQ PROTECTION DES DONNÉES ET RGPD

1) À qui s'adresse le RGPD?

Le RGPD est applicable directement dans tous les pays de l'UE et de l'EEE. Il est valable dans les pays tiers en dehors de l'UE et de l'EEE (p. ex. Suisse, USA) sur la base du principe dit de marché quand des données à caractère personnel de personnes qui se trouvent dans l'UE ou l'EEE sont traitées, et ce dans la mesure où le traitement de ces données est lié à l'offre de marchandises et de prestations de services ou à l'observation du comportement des personnes dans l'UE ou dans l'EEE (p. ex. au moyen de cookies et d'outils de suivi sur un site internet). La nationalité d'une personne et son lieu de résidence ou de séjour ne jouent aucun rôle. Seuls le marché cible ou la présence d'une personne sur ce marché comptent.

En résumé:

- Vous êtes concerné par le champ d'application du RGPD si vous proposez des prestations de services ou des marchandises dans l'UE ou dans l'EEE (valable aussi pour les offres gratuites) ou si votre site internet accessible dans l'UE ou dans l'EEE utilise des cookies, des outils d'analyse, de suivi, etc.

2) Quelles données sont-elles protégées?

Contrairement à la loi fédérale sur la protection des données (LPD), le RGPD ne protège que les données des personnes physiques. La protection de la LPD s'étend également aux personnes morales. La RGPD et la LPD ne s'appliquent pas aux personnes décédées.
Par ailleurs, seules sont protégées les «données à caractère personnel» (RGPD) ou les «données personnelles» (LPD). Sont considérées comme telles toutes les informations et indications se rapportant à une personne identifiée ou identifiable et pouvant être attribuées à une personne spécifique.

En résumé:

- Selon le RGPD, seules les données de personnes physiques spécifiques ou pouvant être spécifiées (nom, numéro d'AVS, adresses IP, données de localisation, etc.) sont protégées.
- Les données de *personnes morales* ne sont pas protégées par le RGPD mais par la LPD.

3) Que signifie le traitement des données?

Le RGPD et la LPD parlent de traitement de données. Ils abordent essentiellement la même chose. La définition du terme est large: est considérée comme traitement toute manipulation de données personnelles effectuée avec ou sans une procédure automatisée, notamment la collecte, la saisie, l'organisation, l'interrogation, la transmission, la diffusion, la sauvegarde, la modification, l'effacement ou la destruction. Le traitement de données doit être conforme à la loi. En principe, seules les données nécessaires à la finalité du traitement en question peuvent être traitées.

En résumé:

- Toute manipulation de données à caractère personnel ne poursuivant pas un but purement privé/familial est considérée comme traitement des données et, est concernée par la protection des données. La LPD protège les données de personnes physiques et morales, le RGPD uniquement celles des personnes physiques.

4) Quels principes s'appliquent au traitement de données personnelles?

Tant selon la LPD que selon le RGPD, les données ne peuvent être traitées que conformément à la loi, en toute bonne foi, selon des fins déterminées et de façon reconnaissable/transparente. Selon le RGPD, le respect des principes doit pouvoir être prouvé (obligation de rendre compte).

Les principes suivants s'appliquent:

Légalité: un traitement des données est légal a) si un consentement existe, b) s'il est nécessaire à l'exécution d'un contrat, c) s'il est nécessaire à l'exécution d'une obligation légale, d) s'il est nécessaire à la préservation d'intérêts vitaux, e) s'il est requis pour l'exécution d'une tâche dans l'intérêt du public ou f) s'il est requis pour la préservation d'intérêts légitimes.

Transparence: le responsable informe de manière précise, compréhensible et transparente sur le nom et les coordonnées de contact du responsable, le but du traitement des données et éventuellement d'autres points tels que la durée de sauvegarde des données, le droit de renseignement ou de suppression.

Affectation: les données ne doivent être traitées que pour le but légitime donné.

Minimisation des données: le traitement des données doit être limité à ce qui est nécessaire pour le but donné («aussi peu que possible, autant que nécessaire»).

Exactitude: les données traitées doivent être exactes et à jour si nécessaire. Les données erronées doivent être immédiatement supprimées ou corrigées.

Limitation de la sauvegarde: la sauvegarde des données doit être effectuée dans une forme qui ne permet l'identification de la personne concernée que pendant la durée requise pour atteindre l'objectif.

Sécurité des données: les données personnelles doivent être protégées des traitements non autorisés ou illicites.

En résumé:

- Si vous avez jusqu'à maintenant déjà tenu compte des principes de protection des données lors du traitement des données, le RGPD n'apporte globalement rien de nouveau dans ce domaine.
- Seules les données nécessaires au but concerné peuvent être traitées.

5) Quels sont les droits de la personne concernée?

D'après la LPD et le RGPD, la personne concernée a notamment un droit de renseignement ainsi qu'un droit de rectification ou de suppression de données erronées ou plus nécessaires.

En résumé:

- **Droit de renseignement:** la personne concernée peut notamment demander si des données personnelles sur elle ont été traitées et si tel est le cas, de quelles sources elles proviennent et dans quel but.
- **Droit de rectification:** la personne concernée peut exiger la rectification immédiate de données personnelles erronées.
- **Droit de suppression:** la personne concernée peut exiger la suppression des données personnelles si le traitement des données n'est plus nécessaire, si le consentement au traitement des données était la seule justification et est maintenant révoqué, si la révocation est faite selon le RGPD ou si les données sont traitées de manière illicite.

6) Qu'est-ce qu'une déclaration de protection des données?

Toute personne qui traite des données dans le champ d'application du RGPD doit en informer les personnes concernées «de manière précise, transparente, compréhensible et facilement accessible, dans un langage clair et simple». Cette déclaration de protection des données doit notamment comporter le nom et les coordonnées du responsable ainsi que ceux d'un représentant ou d'un préposé à la protection des données éventuels. Par ailleurs, le but du traitement des données, le fondement juridique, les droits de la personne concernée ainsi que, si possible, la durée de sauvegarde des données doivent être indiqués. En règle générale, la déclaration est faite par écrit ou (surtout pour les sites internet ou dans le contact par e-mail) sous forme électronique.

Contrairement à l'obligation de tenir un registre (voir FAQ 7), cette obligation d'information ne dépend pas de la taille de l'entreprise.

En résumé:

- Avec la déclaration de protection des données, l'entreprise traitant les données respecte son obligation d'information vis-à-vis de la personne concernée, conformément au RGPD.
- L'obligation d'information inclut notamment les coordonnées, le but du traitement des données, la base juridique et les droits de la personne concernée.

7) Quels documents sont-ils requis d'après le RGPD?

D'après le RGPD, toute personne qui traite des données personnelles doit tenir un registre sur ses activités de traitement. Ce registre doit comporter les indications suivantes: a) nom et coordonnées du responsable du traitement, b) but du traitement des données, c) description de la catégorie de la personne concernée et des données, d) catégorie des destinataires éventuels des données, e) le cas échéant transmission à un pays tiers f) si possible délais de suppression des différentes catégories de données et g) si possible description générale des mesures techniques et organisationnelles portant sur la sécurité des données.

Article PME: l'obligation de tenir un registre ne s'applique pas si

- L'entreprise emploie moins de 250 employés.
- Le traitement des données ne représente pas un risque pour les droits de la personne concernée.
- Le traitement n'a lieu que de manière occasionnelle.
- Aucune catégorie de données particulière n'est concernée.

En résumé:

- L'obligation de tenir un registre des activités de traitement ne s'applique pas aux entreprises de moins de 250 employés.

- Le RGPD fixe uniquement le contenu du registre et non sa forme. Sont envisageables tant des présentations sous forme de tableaux que des explications sous forme de texte ou des combinaisons des deux. Le registre est souvent tenu en tant que partie d'une directive de protection des données ou d'un concept de protection des données. L'important est que ce document soit constamment mis à jour.

PROTECTION DES DONNÉES DANS LA BRANCHE FIDUCIAIRE
DOMAINE THÉMATIQUE 1: SITES INTERNET / NEWSLETTER / MÉDIAS SOCIAUX

1) Applicabilité du RGPD

Le RGPD s'applique quand des entreprises d'états tiers comme la Suisse proposent leurs prestations de services ou produits dans l'UE ou dans l'EEE ou quand elles observent le comportement de personnes dans l'UE ou dans l'EEE. Les sites internet et les offres proposées par le biais des sites internet constituent donc un point d'ancrage fréquent de soumission au RGPD. D'un côté, une entreprise peut proposer ses prestations de services et produits par le biais de sites internet également dans l'UE et dans l'EEE. De l'autre, la plupart des sites internet utilisent aujourd'hui des cookies ainsi que des outils de suivi et d'analyse servant à observer le comportement des utilisateurs.

D'après l'état actuel des connaissances, l'accessibilité d'un site internet dans l'UE ou dans l'EEE ne débouche pas en soi sur l'applicabilité. Toutefois, dès qu'une offre est faite (aussi) pour des clients dans l'UE ou dans l'EEE, que les prix sont indiqués en euros ou que des domaines sont utilisés dans l'UE ou dans l'EEE, ceci indique une offre ayant l'EU/l'EEE pour marché cible et par conséquent le RGPD s'applique. le RGPD est applicable dès que le site internet collecte des données sur des visiteurs provenant de l'UE ou de l'EEE.

2) Autorisation du traitement des données dans le domaine des sites internet / newsletter / médias sociaux

Étant donné qu'il n'existe pas de relations contractuelles avec les visiteurs du site internet concerné, ceux-ci doivent être informés de l'utilisation de cookies ainsi que d'outils de suivi et d'analyse, et la personne concernée doit donner son accord (les cases qui sont déjà cochées ne sont pas autorisées). Le consentement doit pouvoir être prouvé et la personne concernée peut le révoquer à tout moment (p. ex. dans le cas des newsletters). Pour les entreprises fiduciaires le plus grand besoin d'agir se trouve parfois dans le domaine des sites internet / newsletter / médias sociaux

3) Minimisation des données

Seules les données nécessaires au but concerné peuvent être traitées. C'est pour cette raison qu'il faut justement définir le but poursuivi dans le domaine des sites internet / newsletter / médias sociaux. Trop de données ont tendance à être collectées. Ainsi, p. ex., il n'est pas nécessaire, en règle générale, d'indiquer la date de naissance d'une personne, l'adresse postale ou le nom pour recevoir une newsletter électronique non personnalisée.

4) Protection de la vie privée par défaut et protection de la vie privée dès la conception (privacy by default and privacy by design)

Les sites internet doivent être conçus de telle sorte que grâce à des préréglages techniques, la protection des données des visiteurs soit la plus grande possible. Le RGPD exige « la protection des données par la conception technique et par des paramétrages par défaut conformes à la protection des données » (protection de la vie privée par défaut et protection de la vie privée dès la conception). Déjà lors de la planification du traitement des données, l'entreprise doit garantir, grâce à des mesures techniques et organisationnelles appropriées, que seules les données qui sont nécessaires au but en question sont traitées et que les principes de protection des données sont mis en œuvre efficacement.

5) Conservation et suppression des données

Les données ne doivent être conservées que tant que cela est nécessaire pour le but fixé. Les données qui ne sont plus nécessaires doivent être supprimées. Si des données sont traitées pour l'envoi d'une newsletter électronique, elles doivent p. ex. être supprimées si la personne concernée ne souhaite plus recevoir la newsletter.

6) Déclaration de protection des données selon le RGPD

La déclaration de protection des données portant sur le traitement des données par le biais d'un site internet doit pouvoir être consultée gratuitement et facilement sur le site en question. Elle doit notamment comporter le nom et les coordonnées du responsable (entreprise fiduciaire) ainsi que ceux d'un représentant ou d'un préposé à la protection des données éventuels. Par ailleurs, le but du traitement des données, le fondement juridique, les droits de la personne concernée ainsi que, si possible, la durée de sauvegarde des données doivent être indiqués.

7) Registre sur les activités de traitement selon le RGPD

Toute personne qui est concernée par le champ d'application du RGPD doit tenir un registre sur toutes les activités de traitement effectuées dans le domaine correspondant. Ce registre contient le nom et les coordonnées du responsable (entreprise fiduciaire et, le cas échéant, le préposé interne à la protection des données), le but du traitement, une description de la catégorie des personnes concernées (visiteurs du site internet), la catégorie des destinataires auxquels sont communiquées les données à caractère personnel, si possible les délais prévus pour la suppression des catégories de données, de même qu'une description générale des différentes catégories de données.

Article PME: l'obligation de tenir un registre ne s'applique pas si

- L'entreprise emploie moins de 250 employés.
- Le traitement des données ne représente pas un risque pour les droits de la personne concernée.
- Le traitement n'a lieu que de manière occasionnelle.
- Aucune catégorie de données particulière n'est concernée.

8) Plus d'informations: Institut 4.0 de FIDUCIAIRE|SUISSE

Guide pratique et autres informations:

Les exigences qui découlent du RGPD dans le domaine des sites internet / newsletter / médias sociaux ainsi que leur mise en œuvre peuvent être, selon les cas, très complexes au niveau juridique et technique. C'est pourquoi l'Institut Fiduciaire 4.0 a élaboré un guide pratique complet qui aborde dans le détail les points mentionnés plus haut et d'autres thèmes (p. ex. share buttons, formulaires de contact, social login, etc.) et fournit des check-lists et des conseils utiles de mise en œuvre. Le guide pratique est disponible sur le site internet de l'Institut Fiduciaire 4.0 (www.fiduciaire40.ch). Par ailleurs, l'Institut Fiduciaire 4.0 se tient volontiers à votre disposition en cas de questions.

DOMAINE THÉMATIQUE 2: PERSONNEL

1) Applicabilité du RGPD

Le traitement de documents de candidature et la gestion d'un dossier personnel sont considérés comme un traitement de données et sont soumis au RGPD et à la LPD. Tant que l'employeur et l'employé se trouvent en Suisse et que le traitement des données (dossier personnel) est effectué en Suisse, le RGPD ne s'applique pas. Dès que l'employé se trouve dans l'UE ou dans l'EEE, l'interprétation de la notion d'offre de services joue un rôle central. Car dès que le traitement des données de l'employeur est lié à l'offre d'une prestation de service dans l'UE ou dans l'EEE, le RGPS s'applique à l'employeur suisse et à son traitement des données.

La notion de prestation de service est large et actuellement, il est difficile de dire ce qui est considéré comme prestation de service ou pas, ce qui donne lieu à des controverses. Ainsi, il n'est pas clairement défini si le simple paiement du salaire dans l'UE ou dans l'EEE suffit (plutôt pas selon l'avis exprimé ici). Mais par exemple, la mise à disposition d'un véhicule d'entreprise à des fins privées dans l'UE ou dans l'EEE pourrait être qualifié de service.

2) Autorisation du traitement des données dans le processus de recrutement et dans les rapports de travail

Les principes de protection des données doivent être respectés tant dans le processus de recrutement que dans les rapports de travail. En particulier, tant selon la LPD que selon le RGPD, seules les données personnelles nécessaires au recrutement ou au traitement des rapports de travail peuvent être traitées.

Processus de recrutement:

- En règle générale, la personne concernée doit approuver le traitement des données. La remise d'un dossier de candidature est considérée comme étant un consentement au traitement des données à des fins de recrutement.

- Dans le processus de recrutement, seules les données personnelles nécessaires pour établir si l'employé potentiel est qualifié et s'il convient pour le poste à pourvoir peuvent être collectées. Ainsi, les données suivantes ne sont généralement pas recueillies au stade du recrutement : numéro d'AVS, numéro de compte, environnement familial, etc.

Rapports de travail:

- Le traitement des données («tenue d'un dossier personnel») est conforme à la loi dans la mesure où il est nécessaire à l'exécution du contrat de travail concret et au respect des obligations légales qui en résultent (finalité).

- Dans les rapports de travail, les données personnelles qui sont nécessaires pour le respect de l'obligation légale (p. ex. temps de travail, absences en raison de maladie, numéro d'AVS), pour la gestion des ressources humaines (p. ex. date de naissance, état civil, coordonnées bancaires) ou pour l'organisation du travail (p. ex. jours de congé, absences planifiées, maladies/incompatibilités) peuvent être collectées.

3) Minimisation des données et sécurité des données

Le dossier personnel ne peut contenir que des données personnelles qui sont nécessaires au traitement des rapports de travail concrets (y c. stade pré- et post-contractuel). Les données personnelles qui ne sont pas (plus) pertinentes (p. ex. vieux avertissements de l'employé) doivent être supprimées.

Les dossiers personnels gérés par voie électronique doivent être protégés de l'accès par des personnes non autorisées et d'un traitement non autorisé et illicite ou d'une perte par le biais de mesures techniques et organisationnelles appropriées.

4) Conservation et suppression des données

Les données ne doivent être conservées que tant que cela est nécessaire pour le but fixé. Dans le processus de recrutement, il faut supprimer les données dès qu'il est établi que le candidat en question n'obtient pas le poste ou ne l'acceptera pas. Les dossiers personnels devraient faire l'objet d'un contrôle régulier afin de voir si les données qu'ils contiennent sont encore nécessaires ou non. Les données qui ne sont plus nécessaires doivent être supprimées. Après le départ de l'employé, seules les données qui sont nécessaires pour traiter les prétentions post-contractuelles ou s'en défendre sont conservées.
L'employé peut exiger la suppression des données si ces dernières ne sont plus nécessaires au but pour lequel elles ont été collectées ou si elles ont été traitées de manière illicite. L'employeur n'est pas tenu de supprimer les données dans la mesure où le traitement est nécessaire pour l'exécution du contrat ou pour la revendication, l'exercice ou la défense de droits.

5) Déclaration de protection des données selon le RGPD

La déclaration de protection des données portant sur le traitement des données pour la gestion du personnel doit, en règle générale, être fixée par écrit (contrat, règlement, fiches d'information) ou par voie électronique (Intranet). Elle doit notamment comporter le nom et les coordonnées du responsable (employeur) ainsi que ceux d'un représentant ou d'un préposé à la protection des données éventuels. Par ailleurs, le but du traitement des données, le fondement juridique, les droits de la personne concernée ainsi que, si possible, la durée de sauvegarde des données doivent entre autres être indiqués.

6) Registre sur les activités de traitement selon le RGPD

Toute personne qui est concernée par le champ d'application du RGPD doit tenir un registre sur toutes les activités de traitement effectuées dans le domaine correspondant. Ce registre contient le nom et les coordonnées du responsable (employeur et, le cas échéant, le préposé interne à la protection des données), le but du traitement (gestion des ressources humaines), une description de la catégorie des personnes concernées (employés), la catégorie des destinataires auxquels sont communiquées les données à caractère personnel, si possible les délais prévus pour la suppression des catégories de données, de même qu'une description générale des différentes catégories de données.

Article PME: l'obligation de tenir un registre ne s'applique pas si

- L'entreprise emploie moins de 250 employés.
- Le traitement des données ne représente pas un risque pour les droits de la personne concernée.
- Le traitement n'a lieu que de manière occasionnelle.
- Aucune catégorie de données particulière n'est concernée.

DOMAINE THÉMATIQUE 3: CLIENTS

1) Applicabilité du RGPD

La LPD s'applique pour les relations purement internes. Le RGPD s'applique si l'entreprise fiduciaire propose ses marchandises ou prestations de services dans l'UE ou dans l'EEE. Les activités de l'agent fiduciaire sont généralement considérées comme des prestations de services au sens du RGPD. Si la personne concernée (client) est une personne morale, le RGPD ne s'applique pas. Attention: si des données à caractère personnel d'une personne physique sont collectées (p. ex. nom, e-mail et numéro de téléphone de l'interlocuteur), le RGPD s'applique.

2) Autorisation du traitement des données dans une relation client

Dans les rapports entre l'entreprise fiduciaire et les clients, les principes de protection des données doivent être respectés. Seules les données personnelles nécessaires au traitement du mandat concret peuvent être traitées selon la LPD (de personnes morales et physiques) et selon le RGPD (de personnes physiques). Le traitement des données est légitime dans la mesure où et tant qu'il est nécessaire pour l'exécution du contrat ou d'une obligation légale. Un consentement séparé de la personne concernée est obligatoire.

3) Minimisation des données

L'agent fiduciaire ne peut collecter que des données qui sont nécessaires au traitement du contrat concret (y c. stade pré- et post-contractuel). Les données personnelles qui ne sont pas (plus) pertinentes doivent être supprimées ou alors il faut demander le consentement explicite de la personne concernée.

Les collectes de données gérées par voie électronique doivent être protégées de l'accès par des personnes non autorisées et d'un traitement non autorisé et illicite ou d'une perte par le biais de mesures techniques et organisationnelles appropriées.

4) Conservation et suppression des données

Les données ne doivent être conservées que tant que cela est nécessaire pour le but fixé. Les données qui ne sont plus nécessaires doivent être supprimées. Après la fin du contrat, il ne faut conserver que les données pour la conservation desquelles il existe une obligation légale (p. ex. obligations de conservation selon le code des obligations).
Le client peut exiger la suppression des données si ces dernières ne sont plus nécessaires au but pour lequel elles ont été collectées ou si elles ont été traitées de manière illicite. L'agent fiduciaire n'est pas tenu de supprimer les données si, et dans la mesure où, il a une obligation légale ou si un traitement est nécessaire pour la revendication, l'exercice ou la défense de droits.

5) Déclaration de protection des données selon le RGPD

La déclaration de protection des données concernant le traitement des données dans le cadre de l'exécution des contrats avec les clients se fait généralement par écrit (contrat). Si le client l'exige et si son identité est prouvée, l'information peut se faire également à l'oral. La déclaration de protection des données doit notamment comporter le nom et les coordonnées du responsable (entreprise fiduciaire) ainsi que ceux d'un représentant ou d'un préposé à la protection des données éventuels. Par ailleurs, le but du traitement des données, le fondement juridique, les droits de la personne concernée ainsi que, si possible, la durée de sauvegarde des données doivent être indiqués.

6) Registre sur les activités de traitement selon le RGPD

Toute personne qui est concernée par le champ d'application du RGPD doit tenir un registre sur toutes les activités de traitement effectuées dans le domaine correspondant. Ce registre contient le nom et les coordonnées du responsable (entreprise fiduciaire et, le cas échéant, le préposé interne à la protection des données), le but du traitement, une description de la catégorie des personnes concernées (clients fiduciaires), la catégorie des destinataires auxquels sont communiquées les données à caractère personnel, si possible les délais prévus pour la suppression des catégories de données, de même qu'une description générale des différentes catégories de données.

Article PME: l'obligation de tenir un registre ne s'applique pas si

- L'entreprise emploie moins de 250 employés.
- Le traitement des données ne représente pas un risque pour les droits de la personne concernée.
- Le traitement n'a lieu que de manière occasionnelle.
- Aucune catégorie de données particulière n'est concernée.

CHECK-LISTS RGPD POUR LES AGENTS FIDUCIAIRES

APPLICABILITÉ RGPD

RGPD (généralement) pas applicable	RGPD (généralement) applicable
☐ Les employés de l'entreprise fiduciaire viennent de l'UE/EEE avec lieu de travail en CH.	☐ L'entreprise fiduciaire a une filiale, une succursale ou un établissement dans des états de l'UE/EEE.
☐ Le site internet de l'entreprise fiduciaire est uniquement orienté sur le marché suisse et n'utilise pas de cookies, d'outils de suivi et d'analyse, etc. (observation du comportement).	☐ Le site internet de l'entreprise fiduciaire est accessible aux états de l'UE/EEE et utilise des cookies, outils de suivi et d'analyse, etc. (observation du comportement).
☐ L'activité commerciale de l'entreprise fiduciaire est uniquement orientée sur les clients en Suisse.	☐ L'activité commerciale de l'entreprise fiduciaire est aussi orientée sur les clients dans l'UE/EEE.
☐ L'entreprise fiduciaire s'occupe de la comptabilité des salaires/de l'administration des salaires pour des clients en CH ayant des employés venus d'états de l'UE/EEE.	☐ L'entreprise fiduciaire a des clients dans des états de l'UE/EEE par le biais desquels elle traite des données (aussi) de personnes physiques comme les interlocuteurs, adresses e-mail personnelles, etc. (banque de données de clients).
☐ La banque de données de clients de l'entreprise fiduciaire ne contient que des données de personnes physiques ou morales en Suisse ou que des données de personnes morales dans l'UE/l'EEE (pas de données sur l'interlocuteur, adresses e-mail personnelles, etc.).	☐ L'entreprise fiduciaire offre des prestations de services (gratuites) dans des états de l'UE/EEE, comme des conseils, des cours, des newsletters, etc., ou fait la promotion de ses prestations de services dans des états de l'UE/EEE.

LÉGALITÉ DU TRAITEMENT DES DONNÉES RGPD

Au moins l'une des conditions ci-dessous doit être remplie pour que le traitement des données soit légal.

	Condition
☐	**La personne concernée a donné son consentement au traitement pour le but correspondant**. *Ainsi, par exemple, lors de l'usage d'un site internet, l'utilisation de cookies ainsi que d'outils de suivi et d'analyse doit être signalée, et la personne concernée doit donner son accord (les cases qui sont déjà cochées ne sont pas autorisées). Le consentement doit pouvoir être prouvé et la personne concernée peut le révoquer à tout moment.*

☐	**Le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles**. *Le traitement des données de l'entreprise fiduciaire repose régulièrement sur un contrat avec le client (mandat), avec l'employé (contrat de travail) ou, le cas échéant avec un tiers. Il est donc légal.*
☐	**Le traitement est nécessaire à l'exécution d'une obligation légale**. *Les obligations légales pour les entreprises fiduciaires découlent notamment du droit comptable, du droit de la révision ou du droit du travail public (loi sur le travail, y c. ordonnances).*
☐	**Le traitement est nécessaire à la préservation des intérêts vitaux.** *Cette justification devrait être donnée régulièrement lorsque la vie et l'intégrité corporelle d'une personne concernée sont en danger.*
☐	**Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou dans l'exercice de l'autorité publique**. *L'exercice d'une charge publique est envisageable ici.*
☐	**Le traitement est nécessaire à la préservation des intérêts légitimes**. *On peut penser ici à la mise en œuvre ou à la défense de droits.*

BESOIN D'AGIR RGPD

	Besoin d'agir
☐	**Voir si votre entreprise fiduciaire est concernée par le champ d'application du RGPD et si oui, pour quelles activités**. *Souvent, les sites internet et le traitement des données qui en est lié relèvent du champ d'application du RGPD s'ils utilisent des cookies ainsi que des outils de suivi et d'analyse ou s'ils proposent des newsletters.*
☐	**Concevoir des sites internet / newsletter / médias sociaux conformément au RGPD**. *Les sites internet avec coordonnées et déclaration de protection des données sur le type, la forme et le but des données traitées (cookies, outils de suivi et d'analyse, etc.) ainsi que sur les droits des personnes concernées (renseignement, rectification, suppression).*
☐	**Obtenir le consentement de la personne concernée.** *Dans la mesure où la légalité du traitement des données repose exclusivement sur le consentement de la personne concernée, c.-à-d. que la légitimation ne découle pas du contrat ou de la loi, la personne concernée par le traitement des données doit donner son consentement explicitement. Le consentement peut également être donné de manière informelle mais l'entreprise doit pouvoir le prouver. Dans la branche fiduciaire, le consentement est important surtout en lien avec des sites internet / Newsletter / Social Media.*
☐	**Respecter le droit applicable en matière de protection des données (RGPD ou LPD).** *Il s'agit ici de sensibiliser à la protection des données et de prendre conscience des principes de protection des données. Chaque entreprise devrait notamment savoir quelles données elle collecte et dans quel but, et se demander si le volume des données collectées est couvert par le but du traitement des données.*

☐	**Garantir la protection de la vie privée par défaut et la protection de la vie privée dès la conception (privacy by default et privacy by design).** *Le RGPD exige «la protection des données par la conception technique et par des paramétrages par défaut conformes à la protection des données» (protection de la vie privée par défaut et protection de la vie privée dès la conception). Dès la planification du traitement des données, l'entreprise fiduciaire doit garantir, grâce à des mesures techniques et organisationnelles appropriées, que seules les données qui sont nécessaires au but en question sont traitées et que les principes de protection des données sont mis en œuvre efficacement.*
☐	**Rédiger une déclaration de protection des données.** *Le RGDP exige une information «précise, transparente, compréhensible et facilement accessible, dans un langage clair et simple». Doivent être indiqués qui collecte les données, dans quel but et sur quelle base juridique, de même que les droits de la personne concernée.*
☐	**Nommer un représentant au sein de l'UE.** *Les entreprises fiduciaires établies dans les états tiers et pour lesquelles le RGPD est applicables doivent nommer un représentant au sein de l'UE. L'obligation ne s'applique pas si le traitement des données est occasionnel, ne concerne pas de catégorie particulière de données (données sensibles) et ne présente aucun risque pour les droits et les libertés de la personne concernée.*
☐	**Établir un registre des activités de traitement.** *Ce registre doit contenir le nom et les coordonnées de l'entreprise fiduciaire, le but du traitement des données, la description de la catégorie de la personne concernée et des données, etc. L'obligation de tenir ce registre ne s'applique pas aux entreprises fiduciaires de moins de 250 employés (article PME).*
☐	**La personne physique ou morale, l'autorité, l'institution ou l'instance qui décide du traitement des données sont responsables de la protection des données.** *Conformément au droit suisse des sociétés anonymes, le conseil d'administration est responsable de la surveillance suprême des personnes chargées de la direction, notamment en ce qui concerne le respect des lois, des statuts, des règlements et des directives (conformité). Le conseil d'administration peut déléguer la mise en œuvre de la législation en matière de protection des données au niveau opérationnel. Mais il reste responsable du contrôle.*

Pour l'union **FIDUCIAIRE|SUISSE:**

Institut fiduciaire et droit
Monbijoustrasse 20
Case postale
3001 Berne
Téléphone: 031 380 64 30
fiduciaire@fiduciairesuisse.ch
www.fiduciairesuisse.ch

FIDUCIAIRE | SUISSE