Aide à la mise en œuvre de FIDUCIAIRE|SUISSE

Octobre 2022

Les questions et instructions suivantes vous permettront de mettre en œuvre les nouvelles exigences de la loi révisée sur la protection des données dans votre entreprise fiduciaire. Selon la réponse que vous donnez à chaque question pour votre entreprise, soit vous ne devez rien faire, soit vous pouvez suivre les instructions relatives à chaque thème et adapter vos processus, vos directives internes, vos contrats, etc. Vous trouverez des modèles supplémentaires dans l'espace réservé aux membres du site Internet de FIDUCIAIRE|SUISSE.

Ce guide n'a pas la prétention d'être exhaustif et ne constitue pas un conseil juridique. Veuillez également consulter la nouvelle loi et l'ordonnance correspondante et demander conseil à des spécialistes de la protection des données en cas d'autres incertitudes. Vous trouverez de plus amples informations sur la loi sur la protection des données sur le site de l'Office fédéral de la justice : https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

Question	Réponse	Réponse
Avez-vous une **déclaration de confidentialité** à jour pour votre site web, vos contrats, vos confirmations de commande, etc.	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 1
Avez-vous des **directives internes** pour le traitement des données (données clients, données salariales de vos clients, etc.) ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 2
Avez-vous un r**egistre** à jour de tous les traitements de données effectués dans votre entreprise ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 3
Avez-vous une procédure pour répondre en temps utile aux **demandes de renseignements** (par exemple, demande d'accès ou de suppression de données) ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 4
Avez-vous un processus de notification en temps utile d'une **violation** de la protection des données (qui notifie quoi à qui et dans quel délai) ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 5
Avez-vous vérifié auprès des **sous-traitants** ou dans les contrats de ces derniers si la sécurité des données personnelles est garantie, s'ils traitent les données personnelles uniquement comme vous-même et s'ils ont obtenu votre consentement avant de faire appel à un sous-traitant, et ajouté les clauses correspondantes ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 6
Avez-vous un processus de **suppression** ou d'anonymisation de toutes les données personnelles d'une personne concernée ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 7
Vos données sont-elles **stockées exclusivement en Suisse** ? Si non, avez-vous vérifié si ces pays figurent sur la liste du Conseil fédéral et pris d'éventuelles mesures supplémentaires ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 8
Avez-vous fait vérifier si vos processus et votre **infrastructure informatique** répondent à un niveau de sécurité approprié grâce à des mesures techniques et organisationnelles modernes (par ex. directives sur les mots de passe, votre partenaire informatique a-t-il installé les dernières mises à jour, firmwares, etc.)	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 9
Transmettez-vous des **données personnelles sensibles** sans les crypter ?	☐ non vous ne devez rien faire	☐ oui ➔ voir ch.10
Proposez-vous une **communication des données** dans un format électronique courant ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 11
Connaissez-vous le terme **analyse d'impact sur la protection des données** et procédez-vous à de telles analyses en cas de besoin ?	☐ oui vous ne devez rien faire	☐ non ➔ voir ch. 12

1. Déclaration de confidentialité

Avez-vous besoin d'une déclaration de confidentialité sur votre site web ?
Avez-vous besoin d'une déclaration de confidentialité pour vos contrats avec vos clients ?

Étant donné qu'en tant que fiduciaire, vous collectez inévitablement des données personnelles, vous devez informer dans quel but vous traitez des données personnelles, à qui vous les communiquez (pas des noms individuels, mais des catégories de destinataires, par exemple des « sociétés du groupe », des « partenaires », des « prestataires de services informatiques », des « autorités », etc.), si des données sont collectées par des tiers (c'est-à-dire pas par la personne concernée elle-même) et, le cas échéant, lesquelles, et si des données sont envoyées à l'étranger. La formulation d'une déclaration de protection des données - ou de plusieurs déclarations - est donc une tâche principale lors de la préparation à la nouvelle loi.

Lors du respect de l'obligation d'information, la question se pose très souvent de savoir s'il suffit de renvoyer à une déclaration de protection des données sur Internet à partir d'un imprimé - par exemple des CG ou d'une communication écrite. Nous partons du principe qu'une publication sur Internet est suffisante si vous faites au moins référence à la page internet[1].

La personne concernée (par exemple votre client) peut également agir sur les traitements de données par le biais de consentements, en légitimant des traitements qui seraient autrement interdits. Cela n'est toutefois nécessaire qu'à titre exceptionnel, car la LPD et la LPD révisée n'exigent pas de base juridique particulière. Il suffit de respecter les principes de traitement. Un consentement n'est donc nécessaire que si un traitement dépasse le cadre autorisé, par exemple lorsque des données personnelles sensibles sont transmises à des tiers.

Vous pouvez envoyer la déclaration de confidentialité à votre client au moment de l'acceptation du mandat ou l'informer de votre déclaration de confidentialité sur votre site web. Vous pouvez également utiliser des déclarations de confidentialité différentes, par exemple une version uniquement destinée aux visiteurs de votre site web.

Une déclaration de protection des données est-elle nécessaire sur votre site web ? Même si vous ne collectez aucune donnée et que les visiteurs du site ne peuvent pas saisir de données, nous recommandons de publier une déclaration de confidentialité sur votre site web. Si aucune donnée n'est collectée, cela pourrait être mentionné dans la déclaration de confidentialité. Toutefois, les sites web disposent souvent d'au moins un formulaire de contact. Le but est de prendre contact. Un service de formulaire des USA est par exemple intégré à cet effet. Lorsque quelqu'un remplit le formulaire, les données sont enregistrées par ce service de formulaire et vous recevez également les données par e-mail. Les données comprennent les noms et les adresses e-mail ainsi que les messages. S'y ajoutent la date et l'heure ainsi que les adresses IP en tant que métadonnées. Et voilà, vous avez une collection de données et vous les traitez. Vous devez en informer les visiteurs du site web, de préférence dans une déclaration de protection des données.

La déclaration de confidentialité doit notamment contenir les informations suivantes :

- Qui est responsable du traitement des données et comment le contact peut-il être établi ?[2]

[1] voir article spécialisé du Dr David Vasella «La nouvelle loi sur la protection des données et sa mise en œuvre», paru dans le TREX, édition 5/21.
[2] Une adresse e-mail générale est suffisante : protectiondesdonnees@entreprise.ch

- Dans quel(s) but(s) les données personnelles sont-elles traitées ?
- Qui sont les éventuels destinataires des données personnelles traitées et dans quels pays/régions se trouvent-ils ?
- Comment une éventuelle exportation de données est-elle sécurisée ?
- Quels sont les droits des personnes concernées en matière de protection des données ?

2. Directives pour le traitement des données

Nous recommandons d'établir des directives pour le traitement des données au sein de l'entreprise. Les points suivants devraient y figurer :

- Qui a accès* à quelles données ?
- Qui peut traiter quelles données ?
- Où les données doivent-elles être enregistrées ?
- Comment/quand les données sont supprimées
- Quelles données ne peuvent être envoyées que sous forme cryptée ?
- Quelles règles s'appliquent au traitement des données (utilisation de mots de passe, clean desk, etc.) Vous trouverez dans l'espace membres de FIDUCIAIRE|SUISSE d'autres outils sur ce thème.
- Règles spéciales

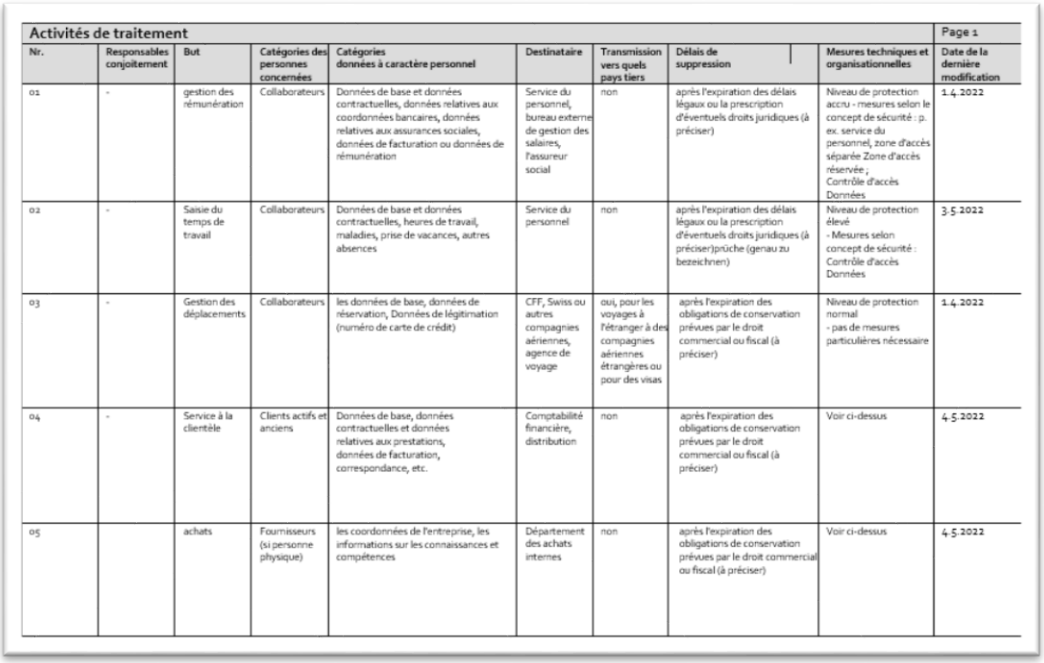
La documentation des processus est utile pour les demandes des autorités ou les éventuelles procédures judiciaires.

*Les droits d'accès doivent être systématiquement tenus à jour dans toutes les solutions logicielles et structures de dossiers. En cas de changement de personnel notamment, la mise à jour doit être prévue dans le processus RH correspondant.

3. Liste de tous les traitements de données

Les entreprises de moins de 250 employés ne sont pas tenues de tenir un registre, sauf s'il existe un risque élevé pour les personnes concernées. Bien que les entreprises fiduciaires ne devraient généralement pas présenter de risque élevé pour les personnes concernées (clients et collaborateurs), nous recommandons de tenir un registre dans tous les cas, car cette vue d'ensemble aide à respecter diverses autres prescriptions de la LPD révisée. Une simple liste Excel ou Word suffit. Vous trouverez un modèle sur le site Internet de FIDUCIAIRE|SUISSE.

Exemple :



Activités de traitement — Page 1

Nr.	Responsables conjoitement	But	Catégories des personnes concernées	Catégories données à caractère personnel	Destinataire	Transmission vers quels pays tiers	Délais de suppression	Mesures techniques et organisationnelles	Date de la dernière modification
01	-	gestion des rémunération	Collaborateurs	Données de base et données contractuelles, données relatives aux coordonnées bancaires, données relatives aux assurances sociales, données de facturation ou données de rémunération	Service du personnel, bureau externe de gestion des salaires, l'assureur social	non	après l'expiration des délais légaux ou la prescription d'éventuels droits juridiques (à préciser)	Niveau de protection accru - mesures selon le concept de sécurité : p. ex. service du personnel, zone d'accès séparée Zone d'accès réservée ; Contrôle d'accès Données	1.4.2022
02	-	Saisie du temps de travail	Collaborateurs	Données de base et données contractuelles, heures de travail, maladies, prise de vacances, autres absences	Service du personnel	non	après l'expiration des délais légaux ou la prescription d'éventuels droits juridiques (à préciser)prüche (genau zu bezeichnen)	Niveau de protection élevé - Mesures selon concept de sécurité : Contrôle d'accès Données	3.5.2022
03	-	Gestion des déplacements	Collaborateurs	les données de base, données de réservation, Données de légitimation (numéro de carte de crédit)	CFF, Swiss ou autres compagnies aériennes, agence de voyage	oui, pour les voyages à l'étranger à des compagnies aériennes étrangères ou pour des visas	après l'expiration des obligations de conservation prévues par le droit commercial ou fiscal (à préciser)	Niveau de protection normal - pas de mesures particulières nécessaire	1.4.2022
04	-	Service à la clientèle	Clients actifs et anciens	Données de base, données contractuelles et données relatives aux prestations, données de facturation, correspondance, etc.	Comptabilité financière, distribution	non	après l'expiration des obligations de conservation prévues par le droit commercial ou fiscal (à préciser)	Voir ci-dessus	4.5.2022
05		achats	Fournisseurs (si personne physique)	les coordonnées de l'entreprise, les informations sur les connaissances et compétences	Département des achats internes	non	après l'expiration des obligations de conservation prévues par le droit commercial ou fiscal (à préciser)	Voir ci-dessus	4.5.2022

4. Demande de renseignements

Les personnes concernées (clients, visiteurs du site web, etc.) disposent de nombreux droits en rapport avec le traitement de leurs données. Elles peuvent faire une demande d'information ou de suppression. Ces demandes doivent recevoir une réponse dans un bref délai (en général dans les 30 jours). Déterminez qui est compétent pour répondre à ces demandes. La liste de tous les traitements de données (point 3) aide à rassembler les informations correspondantes.

Même si l'on ne peut pas s'attendre à ce que de nombreux clients d'entreprises fiduciaires fassent une demande de renseignements, il est néanmoins recommandé de préparer un processus correspondant, y compris un modèle.

Vous trouverez dans le domaine réservé aux membres du site Internet de FIDUCIAIRE|SUISSE un modèle de lettre de réponse.

Votre adresse ...

Votre adresse

Adresse du destinataire

Lieu, date

Octroi de renseignement selon art. 25 LPD

saisir la formule d'appel

En réponse à votre demande de renseignement selon l'art. 25 LPD du date nous répondons par la présente à votre demande dans le délai légal de 30 jours après avoir suffisamment vérifié votre identité.

1. Identité et coordonnée du responsable
[Votre entreprise y compris l'adresse et les données de contact (téléphone, email) Saisir les personnes de contact concernant la protection des données de l'entreprise]

.....
.....
.....

2. Nous avons enregistré les données suivantes vous concernant :
[Ajouter les données personnelles traitées en tant que telles].
.....
.....
.....
.....

Vous trouverez en annexe une copie des traitements de données pertinents.

3. Objet du traitement :
Nous utilisons vos données ci-dessus uniquement dans le but de [saisir l'objet du traitement].

5. Processus notification d'une violation de la protection des données

Il y a violation de la protection des données lorsque des données personnelles sont perdues, effacées, détruites ou modifiées de manière involontaire ou illicite, ou lorsqu'elles sont divulguées ou rendues accessibles à des personnes non autorisées. De telles notifications de violations, qui entraînent pour les personnes concernées un risque élevé d'atteinte à leur personnalité ou à leurs droits fondamentaux, doivent être annoncées le plus rapidement possible (dans l'UE dans les 72 heures) au Préposé fédéral à la protection des données PFPDT. Si le risque est faible, la notification peut être volontaire. Afin de protéger la personne concernée, celle-ci doit également être informée en cas de risque élevé d'atteinte. Les sous-traitants (donc éventuellement les prestataires de services externes) doivent notifier sans délai toute violation de la sécurité des données au responsable du traitement. Des mesures organisationnelles et techniques sont nécessaires pour pouvoir détecter immédiatement une violation de la protection des données. Un registre de tous les traitements de données permet de détecter d'éventuelles violations de la protection des données (point 3).

Vous trouverez sur le site Internet de FIDUCIAIRE|SUISSE un modèle de déclaration au PFPDT.

Formulaire de notification : Violation de la protection des données

En cas de violation de la protection des données avec des données personnelles, veuillez envoyer ce formulaire immédiatement et de manière aussi complète que possible au Préposé fédéral à la protection des données (formulaire de contact ou par courrier : Préposé fédéral à la protection des données et à la transparence, Feldeggweg 1, 3003 Berne). Des informations complémentaires peuvent être transmises ultérieurement ou demandées par le préposé à la protection des données.

1 Informations sur l'organe public responsable

Organe responsable	Cliquez ici pour saisir du texte.
Personne de contact	Cliquez ici pour saisir du texte..
Numéro de téléphone	Cliquez ici pour saisir du texte..
Adresse email	Cliquez ici pour saisir du texte..
Date de la notification	Date
D'autres organes sont-ils impliqués dans le traitement des données	☐ Non ☐ Oui, les suivants : Cliquez ici pour saisir du texte .
Des sous-traitants sont-ils impliqués dans le traitement des données (outsourcing) ?	☐ Non ☐ Oui, les suivants: Cliquez ici pour saisir du texte.

6. Vérifier les contrats avec les sous-traitants / prestataires de services

Pour de nombreuses fonctions, des services de tiers sont utilisés, par exemple pour l'envoi d'e-mails et de newsletters, des logiciels de comptabilité dans le cloud, des fournisseurs de logiciels en tant que service ou pour les vidéoconférences. Vous travaillez probablement vous aussi avec des prestataires de services.

L'externalisation du traitement des données à des sous-traitants est possible si les conditions suivantes sont remplies :

- Il n'y a pas de violation des obligations de confidentialité
- Le sous-traitant ne peut traiter les données que de la manière dont le donneur d'ordre est lui-même autorisé à le faire. Les modifications de finalité ne sont pas autorisées.
- Le sous-traitant doit être en mesure de garantir la sécurité des données.
- Le traitement en sous-traitance ne peut être effectué qu'avec une autorisation préalable.

Vérifier les contrats avec les sous-traitants pour s'assurer que la sécurité des données est garantie et ajouter des clauses appropriées si nécessaire (notamment en ce qui concerne la notification de toute violation de la protection des données). Concernant les clauses, voir également ch. 8.

Nous recommandons également d'inclure une obligation de notification en cas de violation de la protection des données et une obligation d'autorisation en cas de transmission à des sous-traitants.

7. Quand faut-il supprimer les données

Les données personnelles qui ne sont plus nécessaires et pour lesquelles aucun motif justificatif ne peut être prouvé doivent être effacées par l'entreprise. Les données sont correctement effacées lorsqu'elles ne peuvent pas être récupérées sans effort disproportionné.

Vérifiez à l'aide du registre de vos traitements de données (ch. 3) si vous avez prévu un processus de suppression pour tous les traitements de données.

8. Transmission de données à l'étranger

La plupart des fournisseurs de cloud et de logiciels en tant que service (logiciels de comptabilité, newsletters par e-mail, CRM, etc.) ont des serveurs en dehors de la Suisse. Les données personnelles peuvent être communiquées à l'étranger si la législation de l'Etat concerné (ou l'organe international) garantit une protection adéquate. Le PFPDT, ou à l'avenir le Conseil fédéral après la révision de la LPD, tient une liste des « États tiers sûrs », voir la liste des États ici. Pour les « Etats tiers non sûrs », par exemple les Etats-Unis, des clauses contractuelles supplémentaires ainsi que d'autres mesures de sécurité éventuelles sont nécessaires.

En cas d'exportation de données vers les États-Unis (donc aussi d'enregistrement de données personnelles sur des serveurs aux États-Unis), par exemple par l'utilisation d'un service Internet aux États-Unis, une protection des données appropriée peut être garantie par des clauses contractuelles standard, en anglais Standard Contractual Clauses (SCC), ainsi que par d'autres mesures de sécurité éventuelles (anonymisation, cryptage, etc.). Si vous exportez des données vers les États-Unis ou si vous faites appel à des prestataires de services américains, vous devez vérifier s'il est fait référence à de telles clauses contractuelles standard ou si celles-ci sont incluses. Elles font souvent partie des CG ou de la convention de traitement de données. Si ce n'est pas le cas, vous devez faire en sorte que ces clauses soient incluses. Vous devez également évaluer l'utilisation d'éventuelles autres mesures de sécurité dans le cadre d'une évaluation des risques et, le cas échéant, d'une analyse d'impact relative à la protection

des données (AIPD). L'évaluation de l'admissibilité des transferts de données vers les États-Unis peut changer constamment. Veuillez consulter régulièrement la page correspondante du PFPDT.

9. Infrastructure IT

En fonction du risque que présentent les données, des mesures techniques et organisationnelles appropriées doivent être prises. Les données personnelles du service du personnel sont particulièrement délicates et doivent être traitées avec prudence. Les fiduciaires enregistrent également des données sensibles sur les clients et devraient donc accorder une grande importance à la sécurité des données.

Pour garantir la sécurité des données, nous recommandons de faire contrôler l'infrastructure informatique par un spécialiste externe. Celui-ci testera si

- Des mesures organisationnelles sont en place (par ex. directives internes, directives sur les mots de passe, gestionnaire de mots de passe, formation/sensibilisation des collaborateurs, etc.)
- Si tous les logiciels sont à jour avec toutes les mises à jour relatives à la sécurité
- Si tous les appareils sont protégés par des antivirus modernes
- Si des firmwares actualisés sont utilisés
- Si le pare-feu est correctement configuré
- Si les données sont correctement sauvegardées.

Même si vous avez un partenaire informatique externe, vous ne pouvez pas être sûr que tous les points mentionnés ci-dessus sont remplis. De plus, la « fraude »" fait partie des cyberincidents les plus fréquents et le point faible est le facteur humain (mots de passe). C'est là qu'interviennent les mesures organisationnelles et moins les mesures techniques.

FIDUCIAIRE|SUISSE collabore avec des partenaires qui effectuent des contrôles de sécurité pour nos membres. Vous les trouverez sous : https://www.treuhandsuisse.ch/fr/cybersecurite-informations

10. Données personnelles sensibles

Les données personnelles sensibles doivent être particulièrement protégées et toujours transmises sous forme cryptée. Il s'agit entre autres des :

- Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques d'une personne
- De l'appartenance à un syndicat
- Les données génétiques, les données biométriques traitées exclusivement aux fins d'identifier une personne physique de manière univoque
- Les données relatives à la santé
- Les données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne.
- Les données relatives aux poursuites et sanctions administratives ou pénales
- Les données relatives aux mesures d'aide sociale

Les entreprises fiduciaires sont les plus susceptibles d'avoir accès aux données personnelles des deux dernières catégories, de les enregistrer ou de les envoyer.

Les données salariales ne font pas partie des données personnelles sensibles. Il est toutefois recommandé de confirmer que ces données peuvent être envoyées sans être cryptées.

11. Portabilité des données

Avec le droit à la restitution des données, une personne concernée a la possibilité de demander la restitution de ses données personnelles, qu'elle a communiquées à un responsable privé, dans un format électronique courant ou de les faire transmettre à un tiers. La condition est que les données soient traitées de manière automatisée et avec le consentement de la personne concernée ou en relation directe avec un contrat.

Ce droit, qui est probablement plus proche du droit des cartels que du droit de la protection des données, doit faciliter le changement de fournisseur dans l'intérêt de la concurrence. L'avenir nous dira quelle importance il aura dans la pratique.

En tant que membre de FIDUCIAIRE|SUISSE, vous êtes également tenu, en vertu du code de déontologie, de fournir des données sur vos clients.

12. Analyse d'impact relative à la protection des données

Les entreprises doivent dans tous les cas évaluer les risques liés au traitement des données personnelles. Souvent, une évaluation intuitive des risques suffit. Mais certains traitements sont plus délicats. Une réflexion approfondie est alors nécessaire. Si un traitement est susceptible d'entraîner des risques élevés, la LPD révisée exige que le responsable évalue et documente les risques dans le cadre d'une analyse d'impact relative à la protection des données (AIPD).

Il n'est pas toujours facile d'évaluer si les risques sont élevés. Mais une AIPD devrait en tout cas être effectuée lorsque des données personnelles sensibles sont traitées à grande échelle. Il n'est toutefois pas encore question de cela lorsque des données de collaborateurs sont traitées, même si elles contiennent des données personnelles sensibles.