**Nouvelle loi sur la protection des données**
**Recommandations**

**Veuillez noter:** dans les recommandations suivantes, nous renvoyons à chaque fois aux documents de l'Union suisse des arts et métiers (usam) afin que vous puissiez consulter les détails en cas de besoin.

La nouvelle loi sur la protection des données (LPD) constitue, avec la nouvelle ordonnance relative à la loi sur la protection des données (OLPD) et la nouvelle ordonnance sur les certifications en matière de protection de données (OCPD), la nouvelle législation sur la protection des données en Suisse. Cette nouvelle loi vise en premier lieu à renforcer les droits des personnes concernées. Sont considérées comme personnes concernées les personnes dont vous traitez les données pendant que vous êtes considéré comme responsable de ce traitement. Les personnes concernées sont par exemple les clientes et clients et les collaboratrices et collaborateurs.

## Qu'est-ce qui ne change pas?

_ Avec la nouvelle loi sur la protection des données, abrégée LPD, la Suisse ne reprend *pas* le règlement général européen sur la protection des données, abrégé RGPD. En Suisse, le traitement des données personnelles *reste en principe* permis pour autant que certains principes soient respectés. Le principe de base est «ce qui n'est pas interdit est permis» tant que l'information, la transparence et la sécurité des données sont respectées.

En Europe, en revanche, le RGPD n'autorise qu'*exceptionnellement* le traitement des données personnelles. Tout traitement des données personnelles doit être justifié, par exemple avec le consentement des personnes concernées comme des clientes et clients.
→ Mémento, pages 1 et 2

_ Avec la nouvelle LPD, les principes de base suivants *restent* particulièrement importants: sécurité des données, nécessité, licéité, véracité, transparence, finalité. Ainsi, les données personnelles ne peuvent être traitées que tant qu'elles sont nécessaires à la finalité poursuivie. Ensuite, les données personnelles concernées doivent être effacées ou anonymisées.
→ Mémento, pages 2 et 3

_ Avec la nouvelle LPD, le consentement des personnes concernées n'est en principe *toujours pas* nécessaire pour pouvoir traiter leurs données. C'est valable même pour des données personnelles sensibles comme



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch

par exemple les données personnelles relatives à la santé et à la sphère intime. Il n'est donc normalement pas utile de prévoir des clauses sur la protection des données dans les conditions générales (CG), même si l'usam a rédigé un modèle à cet effet. Un tel consentement n'est pas nécessaire et comme il est «caché» dans les CG, il n'est juridiquement pas valable.
→ Mémento, pages 1 et 3; Modèle «clause type de protection des données dans les CGV»

_ Avec la nouvelle LPD, la nomination d'un préposé à la protection des données, appelé en Suisse conseiller à la protection des données, *reste* facultative.
→ Mémento, page 5

_ Avec la nouvelle LPD, des amendes pour violation de la protection des données *continueront* à n'être infligées qu'en cas de faute intentionnelle. La négligence n'est pas punie.
→ Mémento, page 8

_ Avec la nouvelle LPD, il n'y a pas d'introduction de bandeaux pour les cookies comme dans le modèle européen. Nous considérons que l'idée d'introduire des bandeaux pour les cookies, comme le défend l'usam, est erronée.
→ Mémento, page 3

## Quels sont les principaux changements?

_ La nouvelle LPD introduit un devoir *général* d'informer. Il ne suffit plus uniquement que le traitement des données personnelles soit reconnaissable pour les personnes concernées. Les personnes concernées doivent avoir la possibilité de s'informer sur le traitement de leurs données. Par conséquent, chaque responsable doit rédiger une déclaration *générale* de protection des données qui doit normalement être publiée sur le site internet.
→ Mémento, pages 3 et 4

_ Avec la nouvelle LPD, il faut accorder une attention particulière à l'exportation de données et à l'externalisation. L'exportation des données, la transmission de données personnelles dans d'autres pays, et l'externalisation, ou traitement de données personnelles par des tiers mandatés, doivent être protégées par le droit de la protection des données. Un contrat de sous-traitance de traitement des données, en anglais Data Processing Agreement (DPA), est nécessaire pour assurer cette protection.
→ Mémento, page 4



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch

_ Avec la nouvelle LPD, il faut vérifier en cas de violations de la sécurité des données («problèmes de données») s'il existe un devoir d'annonce et/ou d'information. Selon les cas, il faut faire une déclaration au préposé fédéral à la protection des données (PFPDT) et/ou les personnes concernées doivent être informées.
→ Mémento, page 6

_ La nouvelle LPD renforce les droits existants des personnes concernées, par exemple le droit d'accès. Un nouveau droit à la transmission des données est introduit, ça signifie que, sous certaines conditions, les données doivent être remises aux personnes concernées dans le format électronique courant.
→ Mémento, page 7

_ La nouvelle LPD punit davantage de violations de la protection des données et les amendes risquent d'être clairement plus élevées. Les personnes directement responsables risquent une amende personnelle pouvant atteindre 250 000 francs, les entreprises peuvent exceptionnellement être punies d'amendes allant jusqu'à 50 000 francs.
→ Mémento, page 8

_ Avec la nouvelle LPD, le préposé fédéral à la protection des données personnelles et à la transparence, abrégé PFPDT, obtient nettement plus de compétences en tant qu'autorité de surveillance de la protection des données. Le PFPDT peut ouvrir des enquêtes et rendre des décisions. Il peut par exemple ordonner qu'un certain traitement des données personnelles ne soit pas effectué ou que certaines données personnelles soient effacées.
→ Mémento, page 8

_ La nouvelle LPD ne permet plus aux personnes morales, c'est-à-dire essentiellement les entreprises, de prétendre à la protection des données. La nouvelle LPD ne s'applique plus qu'aux personnes physiques en Suisse. Dans la pratique, la protection des données pour les personnes morales n'avait que peu d'importance.
→ Mémento, page 1



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch

## Où faut-il mettre les priorités?

Nous recommandons de mettre la priorité sur la présentation extérieure, la sécurité des données et la prévention des amendes. Nous recommandons donc de donner la priorité aux six étapes suivantes.

**1re étape: Un inventaire des données est-il disponible?**
Pour la mise en œuvre, il est nécessaire de savoir quelles données sur quelles personnes sont traitées pour quoi, comment et où.
Ce registre des activités de traitement qui est introduit avec la nouvelle LPD est volontaire pour la plupart des responsables. Mais il est recommandé de tenir un *inventaire des données.* On peut pour cela s'inspirer des directives relatives au registre sur les activités de traitement. On peut aussi utiliser un mindmap, une fiche mémo ou un outil en ligne.
→ Mémento, pages 4 et 5; Modèle «Registre de traitement des données»

**2e étape: L'externalisation est-elle protégée, en particulier avec un contrat de sous-traitance ?**
Les données sont souvent traitées par des tiers mandatés. On parle de sous-traitance ou d'externalisation. Des exemples typiques sont les services de cloud (sauvegarde des données, plate-formes de marketing et pour newsletter, Microsoft 365 et d'autres logiciels en tant que services, vidéoconférences avec Teams ou Zoom), la comptabilité financière et pour les salaires ou des services d'hébergement.
Dans le cadre d'une telle externalisation, il faut conclure un contrat de sous-traitance de traitement des données, en anglais Data Processing Agreement (DPA), avec chaque fournisseur ou tiers mandaté. Tous les services de cloud ou tous les prestataires d'externalisation proposent de tels contrats de manière standard, souvent dans le cadre des conditions générales (CG). Normalement, il n'est pas possible, en tant que mandataire, d'utiliser son propre contrat en cas d'externalisation.
→ Mémento, page 4; Modèle «Contrat de sous-traitance»

**3e étape: Chaque exportation des données dans des Etats tiers peu sûrs est-elle protégée, en particulier avec des clauses types de protection de données?**
En cas d'externalisation, les données sont souvent traitées *à l'étranger* par des tiers mandatés ou pour d'autres raisons. Si une telle exportation des données se fait dans un Etat tiers non sûr, d'un point de vue de la protection des données, l'exportation des données doit être davantage sécurisée. Presque tous les Etats hors de l'Espace économique européen (EEE) sont considérés comme des Etats tiers non sûrs, dont les Etats-Unis.



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch

Pour la sécurisation, on utilise normalement les clauses types de protection des données, en anglais Standard Contractual Clauses, de la Commission européenne. Tous les services de cloud établis et les autres fournisseurs d'externalisation utilisent par défaut ces clauses types de protection des données.
→ Mémento, page 4

**4e étape: Le devoir d'information est-il satisfait, en particulier avec une déclaration *générale* de protection des données?**
Les personnes concernées doivent être informées des données qui sont traitées dans quel but, comment et où, et de leurs droits, par exemple du droit à l'accès aux renseignements. Le devoir d'information est normalement satisfait avec une déclaration *générale* de protection des données publiée sur le site internet.
La déclaration de protection des données devrait être complète et tenue à jour, par exemple par une actualisation tous les 6 à 12 mois. Pour établir une déclaration de protection des données, on peut utiliser des modèles ou documents-types. Des déclarations de protection des données peuvent être établies en ligne auprès de fournisseurs de générateurs de protection des données.
→ Mémento, pages 3 et 4; Modèle «Déclaration de protection des données»

**5e étape: La sécurité des données est-elle garantie, en particulier avec des MTO?**
La sécurité des données personnelles qui sont traitées doit être garantie avec des mesures techniques et organisationnelles, abrégées MTO. On pense par exemple à la sauvegarde permanente des données, à la mise à jour régulière des logiciels et à la protection de l'accès aux services en ligne (mots de passe uniques et suffisamment longs et authentification avec 2 facteurs) et aux locaux (serrures, listes de clés et autre).
Il faut d'éviter que des personnes non autorisées aient accès à des données personnelles, en particulier à des données sensibles relatives à la santé. Il s'agit également d'éviter que des données soient perdues, par exemple faute d'une sauvegarde efficace.
→ Mémento, pages 3 et 8

**6e étape: Qui s'occupe des demandes des personnes concernées et des devoirs d'annonce et d'information?**
En cas de demandes de personnes concernées, par exemple en cas de demandes d'informations, il est important de réagir à temps et correctement. Le délai se monte à 30 jours mais il peut être prolongé, si nécessaire, avant l'expiration du délai.
Il en va de même pour les éventuelles obligations d'annonce et d'information en cas de «problèmes de données». Il n'y a pas de délai pour cela mais la nouvelle LPD exige de réagir «aussi rapidement que possible».



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch

Il est recommandé de déterminer qui est la personne de contact ou qui sont les personnes de contact pour toutes les questions relatives à la protection des données. Souvent, des demandes de personnes concernées ou des «problèmes de données» impliquent qu'il est nécessaire de faire appel à un spécialiste expérimenté et qualifié.
→ Mémento, pages 6 et 7

L'application de la nouvelle LPD est un processus. La mise en œuvre n'est pas terminée une fois pour toutes mais exige que l'on s'occupe continuellement ou au moins régulièrement de la protection des données. Ainsi, un règlement ou une directive qui documente et systématise la mise en œuvre peut y contribuer. Selon le traitement des données personnelles, une analyse d'impact relative à la protection des données (AIPD) peut exceptionnellement être nécessaire.
→ Mémento, pages 2 et 5; Modèle «Politique de protection des données» et modèle «Analyse d'impact relative à la protection des données»

## Soutien

Le secrétariat de l'ASD ne dispose pas de l'expertise concernant les questions de protection des données. Nous recommandons, en cas d'incertitudes ou de doute, de prendre conseil auprès de spécialistes expérimentés et qualifiés.



**SDV** Schweizerischer Drogistenverband **ASD** Association suisse des droguistes
Thomas-Wyttenbach-Strasse 2 2502 Biel/Bienne Telefon 032 328 50 30 Fax 032 328 50 31 info@drogistenverband.ch
drogistenverband.ch