## Nouvelle loi sur la protection des données
## Réponses aux principales questions

Vous trouverez ci-dessous les réponses aux principales questions relatives à la mise en œuvre de la nouvelle loi sur la protection des données (LPD). Veuillez noter que nous, en tant que secrétariat de l'ASD, n'avons pas d'expertise concernant la nouvelle loi sur la protection des données. Nous vous prions donc d'adresser vos questions à un prestataire spécialisé.

Si vos questions sont d'intérêt général, nous compléterons le présent document, le cas échéant.

| **Questions** | **Réponses** |
|---|---|
| Pourquoi la protection des données est-elle importante? | La protection des données sert à protéger les personnes contre l'utilisation abusive de leurs données en Suisse. Dans ce sens, on pourrait aussi parler de «protection des personnes» plutôt que de «protection des données». |
| Pourquoi y a-t-il une nouvelle législation sur la protection des données en Suisse? | L'actuelle législation sur la protection des données en Suisse a été révisée en premier lieu pour pouvoir continuer à satisfaire aux exigences européennes d'une protection moderne des données. Par rapport au règlement général européen sur la protection des données (RGPD), la Suisse avait pris du retard et risquait de ne plus pouvoir échanger librement des données avec l'Europe. |
| Quels sont les délais transitoires pour la mise en œuvre de la nouvelle LPD? | La nouvelle LPD entre en vigueur le 1er septembre 2023 et doit être mise en œuvre dès cette date. Il n'y a donc pas de délais transitoires dans les faits mais la nouvelle LPD ne sera probablement pas appliquée strictement dès le premier jour. Dans tous les cas, l'application est un processus, car la législation sur la protection des données doit toujours être respectée. Ce n'est pas suffisant de mettre en œuvre la nouvelle LPD une fois pour toutes. |



**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

| **Questions** | **Réponses** |
|---|---|
| Que sont les données personnelles? | Les données personnelles sont des données qui se réfèrent à des personnes identifiées ou identifiables. A l'ère de l'information, il existe de nombreuses possibilités pour qu'une personne soit «identifiable». De manière générale, il est judicieux de partir du principe que toutes les données sont des données personnelles. |
| Que sont les données personnelles sensibles? | Il y a six sortes de données personnelles sensibles:<br>_ les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,<br>_ les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,<br>_ les données génétiques,<br>_ les données biométriques identifiant une personne physique de manière univoque,<br>_ les données sur des poursuites ou sanctions pénales et administratives,<br>_ les données sur des mesures d'aide sociale. |
| Un consentement est-il nécessaire pour le traitement de données personnelles sensibles? | Non, aucun consentement n'est requis. Mais si un consentement est obtenu, il doit être explicite, libre et la personne concernée doit avoir été dûment informée. |
| La nouvelle LPD s'applique-t-elle aussi aux personnes originaires d'Europe? | Oui, la nouvelle LPD s'applique à toutes les personnes en Suisse. Les personnes à l'étranger dont les données sont traitées en Suisse peuvent choisir entre la protection des données du pays concerné et la législation suisse sur la protection des données. |
| La nouvelle LPD ne s'applique-t-elle qu'aux citoyennes et citoyens suisses? | Non, la nouvelle LPD s'applique indépendamment de la citoyenneté. |
| Le règlement général européen sur la protection des données (RGPD) continue-t-il à s'appliquer? | Le règlement général européen sur la protection des données (RGPD) s'applique indépendamment de la nouvelle LPD. Il faut examiner au cas par cas si le RGPD est applicable. Il n'y a pas de lien avec la nouvelle LPD. Le RGPD peut notamment être partiellement applicable si l'offre propre s'adresse également à des personnes à l'étranger, aussi en ligne. |



**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

| **Questions** | **Réponses** |
|---|---|
| Où puis-je trouver la nouvelle législation sur la protection des données? | Loi sur la protection des données:<br>https://www.fedlex.admin.ch/eli/cc/2022/491/fr<br>Ordonnance sur la protection des données:<br>https://www.newsd.admin.ch/newsd/message/attachments/75621.pdf<br>Ordonnance sur les certifications en matière de protection des données:<br>https://www.newsd.admin.ch/newsd/message/attachments/75627.pdf |
| La protection des données doit-elle être mentionnée dans les conditions générales (CG)? | Les CG sont un contrat. Il est également possible d'obtenir des consentements par les CG. Mais de tels consentements ne sont normalement pas nécessaires avec la nouvelle LPD. Il ne faudrait pas «cacher» des consentements obtenus à titre exceptionnel dans les CG. |
| Devrions-nous obtenir volontairement le consentement des personnes concernées? | Non, tant qu'aucun consentement n'est requis, il faudrait y renoncer. |
| Avons-nous besoin d'un préposé à la protection des données? | Non, les préposés à la protection des données, appelés conseillers à la protection des données dans la nouvelle LPD, restent facultatifs en Suisse. |
| Avons-nous besoin d'un bandeau pour les cookies pour notre site internet? | Non, la nouvelle LPD n'introduit pas de bandeau pour les cookies sur le modèle européen. Les bandeaux pour les cookies restent nécessaires uniquement si on est soumis à la directive européenne sur les cookies. Il n'y a pas de lien avec la nouvelle LPD. |
| Comment devons-nous publier notre déclaration de protection des données? | La déclaration de protection des données devrait être publiée sur le propre site internet à la rubrique «Déclaration de protection des données», «Informations sur la protection des données», «Protection des données» ou autre. Un lien vers la déclaration de protection des données devrait figurer en bas de page sur chaque page du site internet. Le terme de «Directive sur la protection des données» ne devrait pas être utilisé car une déclaration de protection des données est une possibilité d'information. «Directive» peut donner l'impression qu'il s'agit d'un contrat. |



**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

| **Questions** | **Réponses** |
|---|---|
| Qu'est-ce qu'un «générateur de politique de confidentialité»? | On appelle «générateurs de politique de confidentialité» des logiciels qui permettent d'établir des déclarations de protection des données. Il y a différents fournisseurs qui respectent aussi la nouvelle LPD. La qualité des fournisseurs est très variable. Ainsi, des fournisseurs allemands promettent dans certains cas de respecter la nouvelle LPD mais c'est rarement vrai. |
| Un contrat de sous-traitance pour le traitement de données doit-il être signé à la main? | Non, un contrat de sous-traitance pour le traitement des données peut être conclu sous forme électronique ou même en ligne. |
| Devons-nous divulguer toutes les données en cas de demande de renseignement? | Non, il n'y a pas de droit absolu d'accès pour les personnes concernées. Il faut soigneusement examiner au cas par cas quelles renseignements sont divulgués. |
| Devons-nous effacer toutes les données en cas de demande de suppression? | Non, il n'y a pas de droit absolu de suppression pour les personnes concernées. Il faut soigneusement examiner au cas par cas quelles données sont supprimées. Ainsi, il pourrait y avoir des obligations légales de conservation, par exemple pour les documents comptables ou en raison de la législation cantonale sur la santé. |
| Pouvons-nous encore envoyer de la publicité par courrier postal? | Oui, la nouvelle LPD ne change rien à cet égard. L'envoi de publicité est en premier lieu régi par la législation sur la concurrence déloyale. |
| Pouvons-nous encore envoyer des newsletter par mail? | Oui, la nouvelle LPD ne change rien à cet égard. Pour des raisons de sécurité juridique, il est recommandé de faire confirmer explicitement l'inscription aux newsletters par mail (procédure «double opt-in»). |
| Qu'est-ce que le PFPDT? | PFPDT est l'abréviation de préposé fédéral à la protection des données et à la transparence. Il s'agit de l'autorité de surveillance en matière de protection des données pour les organes fédéraux et les particuliers en Suisse. Pour les autorités et les organes cantonaux, il existe des autorités de surveillance cantonales. |



**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

| **Questions** | **Réponses** |
|---|---|
| Pour qui le registre d'activités de traitement des données est-il obligatoire? | Les personnes physiques et les entreprises qui emploient moins de 250 collaborateurs ne doivent pas tenir un registre d'activités de traitement des données en Suisse. Mais il y a deux exceptions:<br>_ Si des données sensibles sont traitées à grande échelle.<br>_ Si un profilage à haut risque est effectué.<br>Ces deux exceptions devraient être rares. |
| Pouvons-nous encore utiliser des services de cloud américains? | Oui, mais l'utilisation doit être doublement sécurisée: d'un côté avec un contrat de sous-traitances de traitement des données, en anglais Data Processing Agreement (DPA), et de l'autre côté avec des clauses types de protection des données (CPD), en anglais Standard Contractual Clauses (SCC). Les services de cloud établis proposent ces protections de manière standard. |
| Pouvons-nous encore utiliser Google Analytics? | Oui, comme pour les services de cloud américains en général. Mais il est recommandé d'opter pour des alternatives respectueuses de la protection des données, pour autant qu'on n'ait pas absolument besoin des fonctions de Google Analytics. Friendly Analytics est une alternative possible en Suisse (https://friendly.ch/). |
| Pouvons-nous encore utiliser Google Fonts? | Oui, comme pour les services de cloud américains en général. Mais il est recommandé d'héberger soi-même les polices de caractère, plutôt que de les charger via Google Fonts. |
| Que sont des Etats tiers non sûrs? | Le Conseil fédéral tient une liste d'Etats qui, du point de vue suisse, présentent un niveau de protection des données suffisant. Inversement, tous les autres Etats sont considérés comme non sûrs. «Non sûr» signifie qu'en cas d'exportation des données dans de tels Etats, une protection particulière est nécessaire, en particulier avec les clauses types de protection des données. |
| Y a-t-il des clauses types de protection des données suisses pour l'exportation des données? | Non, les clauses types de protection des données de la Commission européenne sont utilisées, le cas échéant avec des compléments pour la Suisse. |



**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

| **Questions** | **Réponses** |
|---|---|
| A quelle fréquence une déclaration de protection des données doit-elle être actualisée? | Une déclaration de protection des données doit être tenue à jour et complète. Dans la pratique, il est judicieux d'actualiser la déclaration de protection des données au moins une fois par année. |
| Combien de caractères spéciaux un mot de passe sûr devrait-il contenir? | Un mot de passe sûr ne doit pas forcément contenir des caractères spéciaux. Il est en premier lieu important que le mot de passe soit suffisamment long, 12 caractères ou plus, et utilisé une seule fois. Les caractères spéciaux permettent d'augmenter la sécurité du mot de passe. Un gestionnaire de mots de passe permet de créer et de gérer facilement un grand nombre de mots de passe. |
| A quelle fréquence faut-il changer les mots de passe? | Il n'est pas nécessaire de changer régulièrement les mots de passe. Un mot de passe ne devrait être modifié que pour des raisons justifiées, par exemple après un problème de données auprès d'un service en ligne. |
| A quelle fréquence devrions-nous actualiser nos logiciels? | Les logiciels doivent toujours être à jour. La plupart des actualisations comblent aussi des failles de sécurité. |
| Dans quel délai devons-nous réagir aux demandes des personnes concernées? | En principe, le délai est de 30 jours. Il peut être prolongé mais la prolongation doit intervenir avant l'expiration des premiers 30 jours. |
| Quand devons-nous réaliser une analyse d'impact relative à la protection des données? | Une analyse d'impact relative à la protection des données, abrégée AIPD, doit être réalisée au préalable si un traitement peut entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Le cas devrait se produire rarement. |
| Combien de temps les données personnelles doivent-elles être enregistrées? | Les données personnelles doivent en principe être conservées aussi longtemps qu'elles sont nécessaires à la finalité poursuivie. Par ailleurs, il peut également y avoir des obligations de conservation légales, par exemple pour des documents comptables ou en raison de la législation cantonale sur la santé. |



**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

| **Questions** | **Réponses** |
|---|---|
| Y a-t-il un risque d'amendes élevées? | La nouvelle LPD relève les amendes possibles de 10 000 francs à 250 000 francs. En outre, la nouvelle LPD introduit de nombreuses nouvelles infractions pénales. Le risque d'amende augmente donc considérablement. |
| Les employeurs peuvent-ils payer les amendes des employés pour violation de la protection des données? | Non. Mais les employeurs peuvent payer les frais d'avocats et de procédure dans le cadre du devoir d'assistance et de protection juridique. |
| Les amendes pour violation de la protection des données peuvent-elles être assurées? | Non, car pour être punissable, il faut qu'un acte soit intentionnel. L'acte intentionnel n'est pas considéré comme un risque et ne peut donc pas être assuré. |
| Que se passe-t-il si un fournisseur de cloud a son siège à l'étranger mais que les données sont stockées en Suisse? | Un stockage des données en Suisse est utile mais en fin de compte, c'est le siège qui est déterminant. Il faudrait, selon les possibilités, utiliser des fournisseurs de cloud avec des sièges en Suisse ou dans l'Espace économique européen (EEE). Pour Microsoft, par exemple, les contrats pour Microsoft 365 peuvent être conclus avec la filiale irlandaise de Microsoft. |



**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