Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ

FAQ Droit de la protection des données

1er février 2023

1 Décision du Conseil fédéral

1.1 Quelle décision le Conseil fédéral a-t-il prise le 31 août 2022 ?

Le Conseil fédéral a décidé de mettre en vigueur au 1er septembre 2023 la nouvelle loi fédérale sur la protection des données (LPD) et les dispositions d'exécution figurant dans deux nouvelles ordonnances, l'une sur la protection des données (OPDo), l'autre sur les certifications en matière de protection des données (OCPD).

1.2 Pourquoi le nouveau droit de la protection des données n'entre-t-il en vigueur que le 1er septembre 2023 ?

En fixant la date d'entrée en vigueur au 1er septembre 2023, le Conseil fédéral exauce un vœu formulé par l'économie. La période transitoire d'un an laisse suffisamment de temps aux responsables du traitement pour prendre les dispositions nécessaires à la mise en œuvre du nouveau droit.

2 But et contenu du droit de la protection des données

2.1 Quel est le but du droit de la protection des données ?

Le droit de la protection des données concrétise le droit fondamental à l'autodétermination informationnelle inscrit à l'art. 13, al. 2, Cst. Il a pour but de protéger la sphère privée des personnes physiques et d'assurer que ce droit fondamental est réalisé non seulement dans la relation à l'État, mais également dans les relations qui lient les particuliers entre eux (art. 35, al. 3, Cst.).

2.2 Que régit le droit de la protection des données ?

Le droit de la protection des données arrête les principes régissant le traitement de données personnelles. Il définit les obligations de celles et ceux qui traitent des données personnelles et les droits des personnes dont les données sont traitées. Pour garantir que ces règles soient bel et bien appliquées dans la pratique, le préposé fédéral à la protection des données et à la transparence (PFPDT) est chargé de surveiller le respect des prescriptions fédérales dans ce domaine.

3 Modifications essentielles découlant de la révision totale du droit de la protection des données

3.1 Pourquoi une révision du droit de la protection des données était-elle nécessaire ?

La révision du droit de la protection des données s'imposait pour tenir compte des développements technologiques et de la transformation numérique de notre société. Les nouvelles dispositions assurent en outre la compatibilité avec le droit européen et permettent la ratification de la Convention 108+ remodelée du Conseil de l'Europe portant sur la protection des données. Les adaptations apportées au droit de la protection des données sont importantes afin que l'UE continue de reconnaître la Suisse comme un État tiers ayant un niveau adéquat de protection des données et que la communication transfrontière de données reste possible sans exigences supplémentaires. Le nouveau droit vise en particulier à mettre en œuvre les exigences de la nouvelle Convention 108+ du Conseil de l'Europe et de la directive (UE) 2016/680 relative à la protection des données en matière pénale (pertinente pour Schengen), et à permettre l'alignement sur le règlement général de l'UE sur la protection des données (RGPD).

3.2 Que vise la révision totale de la loi sur la protection des données ?

La révision totale vise à renforcer l'autodétermination des personnes concernées au sujet de

leurs données personnelles. Elle apporte notamment les améliorations suivantes :

- amélioration générale de la transparence ;
- renforcement des compétences de surveillance et de l'indépendance du PFPDT ;
- durcissement des dispositions pénales ;
- prise en compte de la protection des données dès la planification du traitement de données (« *protection des données dès la conception* ») et par la définition de règles favorables à la protection des données (« *protection des données par défaut* ») ;
- obligation de procéder à une analyse d'impact relative à la protection des données ;
- droit à la remise ou à la transmission des données personnelles ;
- renforcement de la sécurité des données et notification des violations de la sécurité des données.

La révision doit en outre encourager les responsables à pratiquer l'autorégulation, par le biais de codes de conduite qui faciliteront leur travail et amélioreront l'application de la loi. Ces codes seront élaborés par les associations professionnelles et économiques ou les organes fédéraux et pourront être soumis au PFPDT.

3.2.1 Comment la transparence a-t-elle été améliorée pour les personnes concernées ?

Les personnes physiques doivent pouvoir mieux savoir qui traite leurs données personnelles et à quelles fins afin de faire valoir leurs droits inscrits dans la loi sur la protection des données. À cet effet, on a renforcé d'une part l'obligation des responsables du traitement de pratiquer une information active et d'autre part le droit d'accès des personnes concernées. Une nouvelle obligation d'informer est désormais prévue pour les décisions individuelles automatisées (p. ex. à l'aide d'algorithmes).

3.2.2 Comment l'indépendance et la compétence de surveillance du PFPDT ont-elles été renforcées ?

Le chef du PFPDT (le préposé) sera élu par l'Assemblée fédérale (Chambres réunies). Le PFPDT disposera par ailleurs de son propre budget, ce qui permet de renforcer son indépendance. Ses compétences en matière de surveillance seront étendues. En effet, la nouvelle loi sur la protection des données prévoit que le PFPDT peut, d'office ou sur dénonciation, ouvrir une enquête si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données. Si le PFPDT conclut que des dispositions de protection des données sont violées,

il pourra non seulement émettre une recommandation, mais aussi rendre une décision susceptible de recours. Il pourra par exemple ordonner la modification, la suspension ou la cessation d'un traitement ainsi que l'effacement ou la destruction de données personnelles.

3.2.3 Quels sont les changements dans les dispositions pénales de la loi sur la protection des données ?

Outre un renforcement de la surveillance de la protection des données, le durcissement des dispositions pénales devrait permettre d'améliorer le respect de la loi sur la protection des données. La nouvelle loi sur la protection des données couvre davantage d'infractions et la limite maximale des amendes en cas de violation des prescriptions est passée de 10 000 à 250 000 francs. Les cantons restent responsables de poursuivre et juger les infractions commises. Le PFPDT pourra toutefois dénoncer des infractions aux autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure.

Comme il en était déjà le cas, les dispositions pénales de la nouvelle loi sur la protection des

données visent en premier lieu les personnes physiques, et il ne s'agit pas là d'une exception. En droit suisse, les destinataires des dispositions pénales sont essentiellement des personnes physiques et pas des entreprises. Toutefois, en cas de violation des dispositions de protection des données qui concernent uniquement les entreprises, ce ne sont pas les simples collaborateurs qui seront tenus pour responsables, mais les dirigeants de l'entreprise. Cela signifie que ce sont avant tout les chefs d'entreprise, les organes ou les membres des organes, les associés gérants ainsi que les dirigeants effectifs qui sont responsables. Dans tous les cas, la personne doit disposer d'un pouvoir de décision autonome dans un domaine déterminé de l'entreprise.

3.2.4 Qu'est-ce que l'analyse d'impact relative à la protection des données ?

Celui qui prévoit de procéder à un traitement de données susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées doit en principe procéder à une analyse d'impact relative à la protection des données. On parle de risque élevé lorsque le traitement de données sensibles se fait à grande échelle (p. ex. données concernant la santé) ou en cas de surveillance systématique de grandes parties du domaine public. L'analyse d'impact relative à la protection des données doit comporter une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux des personnes concernées et mentionner les mesures prévues pour protéger sa personnalité et ses droits fondamentaux. Si l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé, il doit en principe obtenir une prise de position du PFPDT.

3.2.5 Qu'est-ce qu'une décision individuelle automatisée et quels sont les droits de la personne concernée dans ce contexte ?

Il y a décision individuelle automatisée lorsqu'une décision est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qu'elle a des effets juridiques sur la personne concernée ou l'affecte de manière significative. En cas de décision individuelle automatisée, tant l'évaluation de la situation sur le fond que la décision elle-même sont faites par une machine ou un algorithme, sans intervention humaine. Pour qu'elle soit considérée comme telle au sens de la nouvelle loi sur la protection des données, la décision doit présenter un certain degré de complexité. Les décisions simples de type « si/alors » ou les questions « oui/non » relatives à des critères objectifs et évidents pour les personnes concernées n'en font pas partie (p. ex. retrait d'argent à partir d'un avoir existant).

La nouvelle loi sur la protection des données prévoit que la personne concernée par une telle décision doit en être informée. Par ailleurs, si elle le demande, elle a la possibilité de faire valoir son point de vue et d'exiger que la décision individuelle automatisée soit revue par une personne physique. Enfin, dans le cadre de son droit d'accès, la personne concernée doit être informée de l'existence d'une décision individuelle automatisée ainsi que de la logique sur laquelle se base la décision.

3.2.6 Qu'est-ce qu'un « profilage » et dans quelle mesure une personne concernée jouit-elle d'une protection accrue ?

Le « profilage » désigne toute forme de traitement automatisé de données personnelles servant à évaluer certains aspects personnels relatifs à une personne physique dans la mesure où il vise à analyser ou à prédire des éléments concernant par exemple le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements d'une personne physique. Pour simplifier, le profilage consiste en une sorte d'appréciation ou d'évaluation d'une personne. L'évaluation

peut consister à analyser certaines caractéristiques de la personnalité, mais elle peut aussi être utilisée pour prédire un comportement ou une qualité future d'une personne. À la différence de la décision individuelle automatisée (voir question 3.2.5), le traitement des données n'est pas forcément entièrement automatisé lors d'un profilage. L'intervention humaine n'exclut pas qu'il s'agisse d'un profilage tant que le traitement des données est pour l'essentiel automatisé. On parle de « profilage à risque élevé » lorsqu'un profilage entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. En d'autres termes, un profilage est à risque élevé lorsque son résultat est un « profil de la personnalité » au sens de la loi sur la protection des données en vigueur jusqu'au 1er septembre 2023. Dans ce cas, il se peut qu'une grande quantité de données (même non sensibles) utilisées pour un profilage permettent de dresser un portrait de la personne concernée, qui, lui, présente un risque accru pour la personnalité et les droits fondamentaux de cette dernière. La personne concernée ne peut souvent avoir aucune influence sur ce « portrait » : elle ne peut ni en contrôler l'exactitude ni l'utilisation.

Les personnes privées sont soumises à des conditions plus strictes lorsqu'elles procèdent à un profilage à risque élevé (exigences plus élevées en ce qui concerne le consentement). Pour les organes fédéraux, des conditions strictes s'appliquent déjà en cas de profilage « classique » : elles ne sont autorisées à procéder à un profilage que si une base légale est prévue dans une loi au sens formel.

3.2.7 Quels sont les tenants et aboutissants du droit à la remise ou à la transmission des données ?

Toute personne concernée peut demander, sous certaines conditions, au responsable du traitement qu'il lui remette, dans un format électronique couramment utilisé, les données personnelles la concernant qu'elle lui a communiquées. Elle peut aussi lui demander de transmettre les données personnelles la concernant à un autre responsable du traitement pour autant que cela n'exige pas des efforts disproportionnés. On appelle cela le droit à la portabilité des données. Cette réglementation renforce en outre la position de la personne concernée en sa qualité de consommatrice autonome de services numériques ainsi que la libre concurrence entre les différents fournisseurs de services.

4 Développements internationaux en matière de protection des données

4.1 Quelle importance revêt la directive (UE) 2016/680 pour la Suisse ?

Cette directive constitue un développement de l'acquis de Schengen que la Suisse a dû reprendre en vertu de l'accord d'association à Schengen. Elle a un champ d'application spécifique et régit le traitement de données par les autorités à des fins de poursuite pénale, d'exécution de sanctions pénales et de prévention des risques sécuritaires.

4.2 Quelle importance revêt le règlement général de l'UE sur la protection des données pour la Suisse ?

Ce règlement se compose de dispositions générales relatives à la protection des données traitées par des particuliers ou des autorités dans les États membres de l'UE. Contrairement à la directive (UE) 2016/680, il ne constitue pas un développement de l'acquis de Schengen et n'est pas directement contraignant pour la Suisse. Cela dit, il s'applique aux entreprises sises en Suisse si elles proposent des marchandises ou des services à des personnes qui se trouvent dans l'un des pays de l'UE ou si elles analysent leur comportement (profilage). Il est par ailleurs important pour la Suisse de continuer d'être reconnue par l'UE comme un État tiers ayant un niveau de protection des données approprié sous le régime du règlement

général.

4.3 Le droit suisse de la protection des données satisfait-il aux normes européennes ?

La Suisse dispose depuis l'année 2000 d'une décision d'adéquation de l'UE reconnaissant un niveau de protection des données équivalent. L'adéquation aux prescriptions européennes en matière de protection des données fait l'objet de vérifications périodiques. Le nouveau droit permet de rapprocher le niveau de protection suisse des standards de l'UE.

4.4 Quelles seraient les conséquences si la Commission européenne venait à conclure que le niveau de protection des données en Suisse n'est pas suffisant ?

En l'absence du maintien de la décision d'adéquation de l'UE, les transmissions de données vers la Suisse ne seraient possibles que si des garanties appropriées étaient prévues ou en cas d'autre situation exceptionnelle. Il en découlerait des obstacles administratifs considérables, qui mettraient un frein au libre flux des données et, partant, à l'innovation, pénalisant ainsi la place économique suisse.

4.5 Où en est la Suisse eu égard à la ratification de la Convention modernisée 108+ du Conseil de l'Europe ?

La Suisse va ratifier le Protocole d'amendement lors de l'entrée en vigueur de la LPD révisée. Cette Convention 108+ entrera en vigueur le 11 octobre 2023, à condition qu'au moins 38 États parties aient adhéré au protocole d'ici là.

4.6 Pourquoi la Suisse doit-elle adhérer à la Convention modernisée 108+ ?

Une cinquantaine d'États, dont la Suisse, ont jusqu'ici ratifié la Convention STE 108 du Conseil de l'Europe. Conclue en 1981, elle est le premier instrument contraignant de droit international en matière de protection des données. Le Conseil de l'Europe a décidé d'adapter la Convention à l'ère numérique. En ratifiant sa version révisée, la Suisse pourra continuer d'afficher un haut niveau de protection des données vis-à-vis de ses partenaires internationaux, ce qui renforcera son économie. La révision totale de la LPD vise une mise en conformité avec les exigences de la nouvelle Convention STE 108, très proches de celles des nouvelles dispositions de l'UE et des initiatives prises par la Suisse.