

Nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT

Sommaire

I.	Introduction	2
II.	Historique et objectifs de la révision	2
1.	Étape 1 : partie Schengen.....	3
2.	Étape 2 : loi complète.....	3
III.	Révision totale de la loi sur la protection des données : principales nouveautés	3
3.	Uniquement les données de personnes physiques	3
4.	Données personnelles sensibles.....	3
5.	Protection des données dès la conception et par défaut	3
6.	Conseillers à la protection des données.....	4
7.	Analyse d'impact relative à la protection des données personnelles	4
8.	Codes de conduite	5
9.	Certifications	5
10.	Registre des activités de traitement	5
11.	Communication de données personnelles à l'étranger.....	5
12.	Devoir d'informer consolidé	6
13.	Droit d'accès de la personne concernée	6
14.	Devoir d'annoncer les violations de la sécurité des données	6
15.	Droit à la portabilité des données personnelles.....	7
16.	Enquête sur toutes les infractions aux prescriptions de protection des données ...	7
17.	Décisions	7
18.	Consultations.....	7
19.	Prises de position spontanées et information du public.....	8
20.	Émoluments.....	8
21.	Sanctions.....	8

I. Introduction

Lors de la session d'automne 2020, l'Assemblée fédérale a adopté la révision totale de la loi fédérale sur la protection des données (LPD) et la modification d'autres lois sur le sujet. Le délai référendaire, fixé au 14 janvier 2021, s'est écoulé sans qu'un référendum ait été déposé. L'administration fédérale est en train de rédiger les ordonnances d'exécution y afférentes. Il est prévu que le Conseil fédéral les mette en vigueur au second semestre 2022, en même temps que la nouvelle LPD.

Le secteur privé et les autorités fédérales devront avoir d'ici là adapté le traitement des données personnelles aux nouvelles dispositions. Le PFPDT met en évidence ci-après les principales nouveautés dont ils devront tenir compte à cette fin.

II. Historique et objectifs de la révision

La première loi fédérale du 19 juin 1992 sur la protection des données est entrée en vigueur à l'été 1993, à une époque où Internet n'était pas encore utilisé à des fins commerciales et où rien ne laissait présager la réalité numérique d'aujourd'hui caractérisée par l'omniprésence des smartphones. Après une révision partielle en 2008, qui avait pour but de mieux informer la population sur le traitement de ses données, il est rapidement apparu que le développement technologique fulgurant rendait d'autres adaptations nécessaires. Il est quasiment impensable aujourd'hui, pour la majeure partie de la population, de se passer d'un accès permanent à Internet et d'appareils intelligents dotés d'écrans tactiles. Une refonte globale de la LPD était donc devenue inévitable pour garantir à la population une protection adéquate des données dans un quotidien marqué par le *cloud-computing*, le *big data*, les réseaux sociaux et l'Internet des objets.

À l'automne 2017, le Conseil fédéral a approuvé le projet d'une révision totale de la loi, puis l'a transmis aux chambres fédérales, accompagné du message y afférent. Cette révision avait pour objectif d'adapter la protection des données aux évolutions technologiques et sociales. La nouvelle LPD devait donc satisfaire à cette exigence : renforcer l'autodétermination en matière informationnelle et la sphère privée des citoyens et ainsi garantir ces dernières le plus longtemps possible.

Outre le renforcement des droits des personnes concernées, le Conseil fédéral met en avant, dans son message, une approche fondée sur le risque comme premier principe de la révision, approche selon laquelle l'État et les entreprises doivent déceler à temps les risques pour la sphère privée et l'autodétermination informationnelle et intégrer dès la conception de leurs projets numériques les exigences relatives à la protection des données. Les risques élevés et les mesures techniques et organisationnelles visant à les écarter ou à les atténuer doivent être documentés. La LPD révisée encourage également l'autorégulation, dans la mesure où les membres des branches qui édictent un code de conduite contraignant sont dégagés de certaines obligations. Enfin, elle contient diverses nouveautés destinées à renforcer les pouvoirs de surveillance du PFPDT.

Le Parlement a décidé, début 2018, de scinder la révision en deux étapes. Dans un premier temps et afin de respecter les délais de mise en œuvre fixés dans le droit international, les dispositions concernant les traitements des données applicables aux organes fédéraux (comme fedpol) qui mettent en œuvre la directive (UE) 2016/680 modifiée relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le domaine du droit pénal ont été adaptées. Ces dispositions constituent en effet un développement de l'acquis de Schengen. Les travaux ont abouti à la LPD Schengen, ou LPDS. La révision totale de la LPD dans son intégralité s'est déroulée dans un second temps.

1. Étape 1 : partie Schengen

La LPDS est entrée en vigueur le 1^{er} mars 2019. Sa durée de validité court jusqu'à l'entrée en vigueur de la révision totale. D'autres lois qui concernent la coopération Schengen en matière pénale ont ensuite été adaptées.

2. Étape 2 : loi complète

Conseil prioritaire, le Conseil national s'est attelé à la révision totale de l'ensemble de la loi lors de la session d'automne 2019, révision que les chambres fédérales ont adoptée le 25 septembre 2020 après élimination des divergences. En rédigeant la nouvelle LPD, le Conseil fédéral et le Parlement ont tenu compte de l'amendement de la Convention 108 du Conseil de l'Europe¹, que la Suisse a signé, ainsi que du règlement général de l'UE sur la protection des données (RGPD)². Ce dernier, en raison de son champ d'application extraterritorial, est déjà appliqué par une grande partie de l'économie suisse depuis son entrée en vigueur en mai 2018. Malgré cet adossement au droit européen, la nouvelle LPD s'inscrit dans la tradition juridique suisse puisqu'elle présente un degré élevé d'abstraction et est formulée de manière technologiquement neutre. Elle s'écarte du RGPD non seulement par sa brièveté, mais aussi par une terminologie en partie divergente. La Suisse et l'UE, après le renouvellement de leur législation relative à la protection des données, devraient reconnaître réciproquement l'équivalence de leur niveau de protection des données, si bien que l'échange informel de données personnelles restera possible par-delà les frontières. La décision européenne de reconnaissance à l'égard de la Suisse, qui date de l'an 2000, devrait être renouvelée au printemps 2021.

III. Révision totale de la loi sur la protection des données : principales nouveautés

3. Uniquement les données de personnes physiques

La LPD révisée vise exclusivement à protéger la personnalité des personnes physiques qui font l'objet d'un traitement de données. Elle ne concerne dorénavant plus les données des personnes morales (sociétés commerciales, associations, fondations, etc.), son champ d'application recouvrant ainsi celui du RGPD. Les entreprises, comme jusqu'ici, pourront toujours se référer à la protection de la personnalité prévue par l'art. 28 du code civil, à la protection du secret commercial et de fabrication prévue à l'art. 162 du code pénal et aux dispositions pertinentes de la loi fédérale contre la concurrence déloyale et de celle sur les cartels.

4. Données personnelles sensibles

L'actuelle définition des données personnelles sensibles est étendue aux données génétiques et aux données biométriques si ces dernières identifient une personne physique de manière univoque.

5. Protection des données dès la conception et par défaut

Les principes de « Privacy by Design » (protection des données dès la conception) et de « Privacy by Default » (protection des données par défaut) sont nouvellement inscrits dans la

¹ Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, conclue à Strasbourg le 28 janvier 1981, approuvée par l'Assemblée fédérale le 5 juin 1997. Les chambres fédérales ont approuvé l'amendement de la convention à l'été 2020. Le Conseil fédéral ne pourra le ratifier qu'une fois que la nouvelle LPD sera entrée en vigueur.

² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

LPD révisée. Ils contraignent les autorités et les entreprises à mettre en œuvre dès la conception des projets les principes de traitement prévus par la LPD en prenant des mesures de protection techniques et organisationnelles appropriées. Selon le principe de la protection des données dès la conception, elles devront concevoir leurs applications de sorte que, entre autres, les données soient systématiquement anonymisées ou effacées. La protection des données par défaut, quant à elle, préserve les utilisateurs d'offres en ligne privées qui n'examinent pas les conditions d'utilisation ni les droits d'opposition qui en découlent : seules sont traitées les données absolument nécessaires à la finalité poursuivie tant que les utilisateurs ne deviennent pas actifs et n'autorisent pas de traitement plus poussé. Afin de garantir cette protection prévue par la nouvelle loi, les entreprises suisses devront vérifier leurs offres à temps et, si nécessaire, procéder à des modifications en utilisant des programmes conviviaux et respectueux de la protection des données.

6. Conseillers à la protection des données

En vertu de l'art. 10 de la LPD révisée, une entreprise privée pourra désigner un conseiller à la protection des données, lequel pourra, mais ne devra pas, être lié à elle par un contrat de travail. Dans les deux cas, l'activité de conseil sera séparée des autres tâches de l'entreprise. Il est aussi recommandé de ne pas mélanger les dossiers du conseil sur la protection des données avec ceux des autres activités de conseil et de représentation juridique. Les conseillers devront par ailleurs pouvoir porter leur point de vue à la connaissance de la direction de l'entreprise en cas de divergence d'opinion. Au contraire du RGPD européen, la désignation d'un conseiller restera facultative pour les personnes privées ; seuls les organes fédéraux en seront légalement tenus. Le conseiller sera non seulement l'interlocuteur à l'interne en matière de protection des données mais aussi l'intermédiaire avec la protection des données administrative et le premier contact du PFPDT. Outre le conseil général et la formation de l'entreprise en matière de protection des données, il aura pour tâche de participer à l'élaboration et à l'application de conditions d'utilisation et de dispositions de protection des données. Si le conseiller interne exerce sa fonction de manière indépendante et sans recevoir d'instruction et s'il n'exerce pas de tâches incompatibles avec sa fonction, l'entreprise pourra, après avoir effectué une analyse d'impact relative à la protection des données, se fonder uniquement sur le conseil interne même si un risque élevé persiste, sans avoir à consulter le PFPDT (cf. ci-dessous « Analyse d'impact relative à la protection des données personnelles »).

7. Analyse d'impact relative à la protection des données personnelles

Les analyses d'impact ne sont pas nouvelles dans le droit suisse sur la protection des données, et les organes fédéraux y sont déjà tenus. Si le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, l'art. 22 de la LPD révisée prévoit que le responsable du traitement privé devra désormais également procéder au préalable à une analyse d'impact. L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe surtout lorsqu'un profilage à risque élevé ou un traitement à grande échelle de données sensibles est prévu. Lorsqu'un système, un produit ou un service est certifié (art. 13 de la LPD révisée) ou lorsqu'un code de conduite reposant sur une analyse d'impact est observé (art. 11), il sera possible de renoncer à établir une telle analyse. S'il ressort d'une analyse d'impact que le traitement envisagé présente encore, malgré les mesures prévues par le responsable du traitement, un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement consultera le PFPDT préalablement au traitement (art. 23 de la LPD révisée). Au cas où le PFPDT aurait des objections concernant l'analyse d'impact elle-même, il suggérera au responsable du traitement des précisions ou des ajouts. Ce devrait surtout être le cas lorsque le texte est si général qu'il ne décrit qu'insuffisamment les risques prévisibles ou les mesures. Si les objections concernent le traitement envisagé en soi, le PFPDT proposera des mesures de modification appropriées au responsable du traitement (cf. ci-dessous « Consultations »). Contrairement aux codes de conduite, les prises de position du

PFPDT ne devront pas être publiées. En leur qualité de documents officiels toutefois, elles seront soumises à la loi sur la transparence. Le responsable du traitement privé pourra renoncer à consulter le PFPDT s'il a consulté à l'interne son conseiller à la protection des données (cf. ci-dessus « Conseillers à la protection des données »).

8. Codes de conduite

À l'art. 11, la nouvelle LPD incite les associations professionnelles, sectorielles et économiques à rédiger leur propre code de conduite et à le soumettre au PFPDT afin qu'il prenne position. Ces prises de position seront publiées. Elles pourront contenir des objections ou suggérer des modifications ou des précisions. Un avis positif du PFPDT justifiera la présomption légale que le comportement défini dans le code est conforme à la protection des données. Les codes trop généraux n'exonéreront toutefois pas des risques qui ne sont pas détaillés dans le texte. S'ils sont soumis à un code de conduite, les membres d'associations pourront être dispensés de l'élaboration d'aides et de directives propres pour l'application de la nouvelle LPD. Autre avantage pour eux de cette forme d'autorégulation : ils ne devront pas effectuer d'analyse d'impact s'ils observent un code de conduite reposant sur une analyse d'impact déjà effectuée et toujours actuelle, prévoyant des mesures de protection de la personnalité et des droits fondamentaux et ayant été soumise au PFPDT.

9. Certifications

En vertu de l'art. 13 de la LPD révisée, les fournisseurs de systèmes ou de logiciels de traitement de données personnelles pourront eux aussi, en plus des exploitants, faire certifier leurs systèmes, leurs produits ou leurs services. Une certification permettra par exemple aux entreprises de prouver qu'elles respectent le principe de la protection des données par défaut et qu'elles disposent d'un système de gestion de la protection des données adéquat. Si un responsable du traitement privé utilise un système, un produit ou un service certifié, il sera dispensé d'établir une analyse d'impact relative à la protection des données. Le Conseil fédéral édictera par voie d'ordonnance de plus amples dispositions sur les procédures de certification et sur le label de qualité.

10. Registre des activités de traitement

En vertu de l'art. 12 de la LPD révisée, les responsables du traitement et les sous-traitants tiendront chacun un registre de toutes leurs activités de traitement. La nouvelle loi liste les indications que ce registre devra au moins contenir, lequel devra constamment être à jour. Le Conseil fédéral prévoira dans l'ordonnance des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées. Alors que les organes fédéraux seront tenus de déclarer leur registre au PFPDT, ce ne sera plus le cas, selon le nouveau droit, des personnes privées traitant des données.

11. Communication de données personnelles à l'étranger

Conformément à l'art. 16 de la LPD révisée, des données pourront être communiquées à l'étranger si le Conseil fédéral a constaté que l'État tiers dispose d'une législation assurant un niveau de protection adéquat. Il publiera une liste à cette fin, liste qui a été dressée par le PFPDT selon le droit en vigueur. Si l'État destinataire concerné n'y figure pas, les données pourront cependant toujours être communiquées, comme selon le droit en vigueur, à condition qu'une protection adéquate des données soit garantie d'une autre manière. Par exemple par un traité international, des clauses de protection des données, qui devront être préalablement soumises au PFPDT, ou des règles d'entreprise contraignantes (*binding corporate rules*). Les clauses type déjà approuvées par la Commission européenne en vertu du RGPD seront reconnues par le PFPDT.

Si une communication à l'étranger est prévue – l'enregistrement sur des systèmes étrangers (cloud) étant aussi concerné –, les pays devront être indiqués, peu importe qu'ils offrent ou non un niveau de

protection des données approprié. Ici, la LPD va plus loin que le RGPD. Il faudra aussi indiquer quelles garanties entrent éventuellement en jeu (par ex. clauses contractuelles type européennes) ou à quelles exceptions visées à l'art. 17 de la LPD révisée le responsable du traitement se réfère éventuellement ; là aussi, la LPD s'écarte du RGPD.

12. Devoir d'informer consolidé

Afin d'atteindre l'objectif de transparence visé par la révision, l'art. 19 de la nouvelle LPD consolide le devoir d'informer pour les entreprises. Pour toute collecte envisagée de données personnelles, le responsable du traitement privé devra informer au préalable la personne concernée de manière adéquate, que la collecte de données soit directement effectuée auprès d'elle ou non. L'actuelle LPD ne prévoit ce devoir d'informer que pour les données personnelles sensibles et les profils de la personnalité. Concrètement, l'identité et les coordonnées du responsable du traitement devront être communiquées, de même que la finalité du traitement et, le cas échéant, les destinataires des données personnelles. Autrement que dans le RGPD, des informations devront aussi être fournies sur l'État destinataire et sur les garanties éventuelles d'un niveau approprié de protection des données (cf. en haut, Communication de données personnelles à l'étranger). Les entreprises devront ainsi vérifier et actualiser leur déclaration relative à la protection des données. Le devoir d'informer ne s'appliquera pas aux données personnelles qui ne sont saisies qu'accessoirement ou par hasard. Il sera par ailleurs limité ou supprimé par les nombreuses exceptions mentionnées à l'art. 20. Ce sera par exemple le cas si la personne concernée dispose déjà des informations ou si le traitement des données personnelles est prévu par la loi. Si le traitement entraîne une décision individuelle automatisée, le responsable du traitement, en vertu de l'art. 21, devra informer la personne concernée et lui accorder le droit d'être entendu et celui de vérifier qui lui reviennent.

13. Droit d'accès de la personne concernée

Le droit d'une personne concernée de demander si des données personnelles la concernant sont traitées est consolidé dans la nouvelle LPD. L'art. 25 dresse une liste étendue des informations que le responsable du traitement devra au moins transmettre (par ex. la durée de conservation des données personnelles traitées). Il prévoit également que la personne concernée devra recevoir toutes les informations nécessaires pour qu'elle puisse faire valoir les droits qui lui sont accordés selon la nouvelle LPD et pour que la transparence du traitement soit garantie. Dans certains cas, le responsable du traitement pourra refuser, restreindre ou différer la communication des renseignements, ce que prévoit déjà le droit en vigueur.

14. Devoir d'annoncer les violations de la sécurité des données

En vertu de l'art. 24 de la LPD révisée, le responsable du traitement devra nouvellement annoncer au PFPDT les cas de violation de la sécurité des données entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Cette disposition s'appliquera aussi bien aux responsables du traitement privés qu'aux organes fédéraux. L'annonce au PFPDT devra être faite dans les meilleurs délais. Le responsable du traitement effectuera au préalable une prévision des conséquences possibles de la violation ainsi qu'une première évaluation afin de déterminer s'il pourrait y avoir péril en la demeure, si la personne concernée doit être informée de l'événement et de quelle manière. Même s'il estime que le risque n'est pas élevé, le responsable du traitement pourra faire volontairement une annonce au PFPDT. Seules devront être signalées au PFPDT les violations de la personnalité et des droits fondamentaux, mais pas les cyberattaques déjouées ou impossibles. Le RGPD européen prévoit lui aussi une obligation de notifier aux autorités de protection des données de l'UE et indique des délais concrets. Le seuil d'annonce en vertu du droit européen est d'ailleurs plus bas, puisqu'il s'applique déjà à un risque simple.

15. Droit à la portabilité des données personnelles

Le droit à la remise ou à la transmission des données personnelles prévu à l'art. 28 de la LPD révisée donnera la possibilité à la personne concernée de demander au responsable du traitement privé qu'il lui remette sous un format électronique couramment utilisé les données personnelles la concernant qu'elle lui a communiquées ou de les transmettre à un tiers. Les conditions suivantes devront être réunies : le responsable du traitement traite les données de manière automatisée et avec le consentement de la personne concernée ou en relation directe avec un contrat. La personne concernée pourra faire valoir ce droit gratuitement, sauf si la remise ou la transmission des données exige des efforts disproportionnés. Ce qui pourra être le cas, s'agissant de données de communication, lorsqu'un tri complexe entre les propres propos et ceux de tiers est nécessaire.

16. Enquête sur toutes les infractions aux prescriptions de protection des données

Le PFPDT devra ouvrir d'office une enquête contre un organe fédéral ou une personne privée qui aura enfreint la nouvelle LPD (art. 49, al. 1, de la LPD révisée). L'actuelle LPD prévoit encore la restriction selon laquelle le PFPDT ne peut mener une enquête d'office contre des personnes privées, y compris établissement des faits, que si la méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes. Ce seuil d'intervention, appelé « erreur de système », sera supprimé. Le nouveau droit prévoit toutefois lui aussi que le PFPDT pourra renoncer à ouvrir une enquête lorsque la violation est de peu d'importance (art. 49, al. 2, de la LPD révisée). Comme jusqu'ici, le PFPDT pourra toujours renoncer à engager de premières étapes formelles s'il s'avère, après un premier contact avec le responsable du traitement, que celui-ci reconnaît les insuffisances qui lui ont été signalées et y remédie en temps utile.

17. Décisions

En vertu de l'art. 51, al. 1, de la LPD révisée, le PFPDT pourra mener des procédures conformément à la loi fédérale sur la procédure administrative³ et formellement ordonner à un organe fédéral ou à un responsable du traitement privé la modification, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction des données personnelles. Il pourra par exemple ordonner qu'une entreprise informe les personnes concernées d'une violation signalée de la sécurité des données. Aujourd'hui, il a seulement la compétence de faire des recommandations et d'ouvrir une action en justice auprès du Tribunal administratif fédéral en cas de non-observation de ces dernières.

Un destinataire pourra faire recours contre une décision du PFPDT devant le Tribunal administratif fédéral puis devant le Tribunal fédéral. Le PFPDT aura aussi qualité pour recourir contre les décisions sur recours du Tribunal administratif fédéral (art. 52, al. 3, de la LPD révisée).

18. Consultations

Le PFPDT n'est ni une autorité d'approbation ni un organisme d'homologation des applications, des produits, des réglementations et des projets. La nouvelle loi prévoit cependant à plusieurs reprises que le responsable du traitement devra consulter le PFPDT avant la clôture définitive des travaux et la réalisation des projets. Les codes de conduite et, en cas de risques résiduels élevés, les analyses d'impact devront lui être présentés pour qu'il prenne position. Vu la nature abstraite de ces objets soumis à consultation, les prises de position du PFPDT n'auront généralement pas valeur de décision, et les mesures et charges qu'il recommandera ne feront l'objet d'aucune possibilité de recours. En revanche, si le responsable du traitement ne les respecte pas, il devra s'attendre à ce que des traitements concrets liés à des recommandations du PFPDT fassent ultérieurement l'objet de décisions. Ces décisions pourront aller jusqu'à l'interdiction de traitements entiers, le responsable du

³ Loi fédérale du 20 décembre 1968 sur la procédure administrative (PA), RS 172.021

traitement pouvant toutefois ici recourir aux voies de droit ordinaires de la procédure administrative.

19. Prises de position spontanées et information du public

Excepté les prises de position dans le cadre de consultations formelles, le PFPDT restera libre de s'exprimer spontanément sur des nouvelles technologies, des phénomènes de numérisation ou des pratiques de traitement de certaines branches et de publier ses opinions et estimations. S'il en va de l'intérêt général, il informera le public, comme jusqu'ici suivant le droit en vigueur, de ses mesures et de ses constatations. En vertu de l'art. 57, al. 2, de la LPD révisée, il en ira de même des constatations et des décisions rendues dans le cadre d'enquêtes formelles du PFPDT.

20. Émoluments

L'art. 59 de la LPD révisée liste les prestations pour lesquelles le PFPDT percevra des émoluments auprès des personnes privées. Ce sera par exemple le cas des prises de position concernant les codes de conduite ou les analyses d'impact, de l'approbation des clauses type de protection des données et de celle des règles d'entreprise contraignantes. Les conseils généraux que le PFPDT fournira à des personnes privées seront eux aussi soumis à des émoluments. Le Conseil fédéral réglera les détails au niveau de l'ordonnance.

21. Sanctions

La nouvelle LPD prévoit des amendes de 250 000 francs au plus à l'encontre de personnes privées (art. 60). Seront punis les comportements et les omissions intentionnels, mais pas la négligence. Le non-respect du devoir d'informer, de renseigner et d'annoncer et la violation des devoirs de diligence et celle du devoir de discrétion seront punis sur plainte seulement. L'insoumission à une décision du PFPDT sera en revanche poursuivie d'office. C'est en principe la personne physique responsable qui sera punie. L'entreprise elle-même pourra toutefois nouvellement l'être aussi, à hauteur de 50 000 francs maximum, si l'identification de la personne punissable au sein de l'entreprise ou de l'organisation nécessite des actes d'enquête disproportionnés.

Au contraire des autorités européennes de protection des données, le nouveau droit n'accorde toujours pas de pouvoir de sanction au PFPDT. Les contrevenants seront punis par les autorités cantonales de poursuite pénale. Le PFPDT pourra dénoncer des infractions et faire valoir les droits d'une partie plaignante dans la procédure (art. 65, al. 2, de la LPD révisée), mais il n'aura pas le droit de porter plainte. Autrement que la nouvelle LPD, le RGPD dispose que les sanctions administratives ne sont prononcées qu'à l'encontre de personnes morales. Les autorités européennes de protection des données peuvent condamner des entreprises fautives à des amendes pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

PFPDT, le 9 février 2021