

# PROTECTION DES DONNÉES ET OBLIGATIONS DU RESPONSABLE DU TRAITEMENT PRIVÉ

## Aperçu à la lumière de la nouvelle loi fédérale sur la protection des données

L'Assemblée fédérale a adopté le 25 septembre 2020 la nouvelle loi fédérale sur la protection des données (nLPD). La présente contribution revient sur la saga politico-juridique qui a accompagné la révision de la loi [1] et examine ensuite les obligations auxquelles seront soumis les responsables du traitement du secteur privé dès l'entrée en vigueur de la nLPD, que nous estimons pour courant 2022.

### 1. GENÈSE DE LA NOUVELLE LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES

**1.1 Évaluation de la loi fédérale du 19 juin 1992 sur la protection des données.** Le développement toujours plus rapide des technologies de l'information, tant dans le secteur privé que public, suscite de grands espoirs pour notre qualité de vie, mais comporte également de nombreux risques. C'est pourquoi, à partir de 2010 jusqu'en février 2011, l'Office fédéral de la justice (OFJ) a procédé à une évaluation de la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1). Approuvé par le Conseil fédéral le 9 décembre 2011, le rapport de l'OFJ soulignait l'importance d'adopter de nouvelles mesures législatives en matière de protection des données [2].

Sur cette base, l'OFJ a mis sur pied un groupe d'accompagnement qui a analysé, de septembre 2012 à octobre 2014, l'opportunité de renforcer la législation en vigueur. Les mesures législatives à prendre devaient tenir compte de quatre objectifs selon le Conseil fédéral: assurer la protection des données plus en amont, sensibiliser davantage les personnes concernées face aux risques des nouvelles technologies, améliorer la transparence des traitements de données et améliorer le contrôle et la maîtrise des données [3]. Le groupe d'accompagnement a publié son rapport le 29 octobre 2014, au sein duquel il a détaillé ses conclusions et développé l'esquisse d'une nouvelle loi [4].

**1.2 L'avant-projet du 21 décembre 2016 et sa procédure de consultation.** Le 1<sup>er</sup> avril 2015, le Conseil fédéral a chargé le Département fédéral de justice et police de lui soumettre un avant-projet de loi au plus tard à fin août 2016. Outre les recommandations du groupe d'accompagnement, l'avant-projet devait impérativement prendre en compte les réformes menées à cette époque au sein de l'Union européenne [5] et du Conseil de l'Europe [6].

Le 21 décembre 2016, le Conseil fédéral a envoyé en consultation l'avant-projet de révision totale de la LPD [7] accompagné du rapport explicatif [8]. L'avant-projet apportait des précisions bienvenues à des principes déjà bien acquis et intégrait des nouveautés, à l'instar du concept de protection des données dès la conception et par défaut. La synthèse des résultats de la procédure de consultation a été publiée le 10 août 2017 [9].

**1.3 Le projet du 15 septembre 2017.** Le Conseil fédéral a transmis à l'Assemblée fédérale le 15 septembre 2017 le projet de révision totale de la loi fédérale sur la protection des données [10], ainsi que le Message [11], ouvrant la voie aux travaux parlementaires [12].

**1.4 Travaux parlementaires.** Le projet de loi a été âprement discuté et disputé. D'emblée, la Commission des institutions politiques du Conseil national (CIP-N) a décidé lors de sa



LIVIO DI TRIA,  
DOCTORANT EN DROIT ET  
ASSISTANT DIPLÔMÉ (MLAW)  
À L'UNIVERSITÉ DE  
LAUSANNE



KASTRIOT LUBISHTANI,  
DOCTORANT EN DROIT ET  
ASSISTANT DIPLÔMÉ (MLAW)  
À L'UNIVERSITÉ DE  
LAUSANNE

séance du 11 janvier 2018 de scinder le projet de révision en deux: d'un côté, la transposition de la Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le domaine du droit pénal, nécessaire en vertu des accords de Schengen, et, de l'autre, la révision totale de la LPD. Ce n'est donc que le 24 septembre 2019 que le Conseil national s'est saisi du dossier de la révision totale de la LPD. Si la première partie du projet a rapidement été «liquidée» selon la terminologie parlementaire, il en est allé autrement pour la révision de la LPD. En effet, le projet a fait de nombreux allers-retours entre les deux chambres et les travaux parlementaires sont allés jusqu'en procédure de conciliation, pour aboutir à un vote final le 25 septembre 2020. Ainsi, la nLPD a finalement été adoptée par le Conseil des États à l'unanimité et le Conseil national par 141 voix pour, 54 contre et 1 abstention.

**1.5 Et la suite?** Publié le 6 octobre 2020 dans la Feuille fédérale, le texte final peut encore faire l'objet d'un référendum facultatif au sens de l'art. 141, al. 1, let. a de la Constitution fédérale jusqu'au 14 janvier 2021 [13]. À notre connaissance néanmoins et à l'heure d'écrire ces lignes, aucun acteur n'a annoncé son intention d'attaquer la loi. Pour autant, la nLPD n'entrera pas en vigueur immédiatement à l'expiration du délai référendaire, car une nouvelle ordonnance accompagnant la nLPD devra au préalable être édictée. Selon toute vraisemblance, cette ordonnance devrait être soumise à une consultation au vu de son importance (cf. art. 3, al. 1, let. d de la loi fédérale sur la procédure de consultation). Le travail de rédaction de l'ordonnance a déjà débuté et le texte devrait être publié au début de l'année 2021. Nous estimons, selon les informations à disposition, que les deux textes – loi et ordonnance – devraient donc entrer en vigueur dans le courant de l'année 2022.

## 2. LES OBLIGATIONS FUTURES DU RESPONSABLE DU TRAITEMENT

**2.1 L'absence de délai transitoire pour une mise en conformité.** Le projet du Conseil fédéral contenait des dispositions transitoires concernant les obligations des responsables de traitement et prévoyait un délai de deux ans suivant l'entrée en vigueur de la nouvelle loi pour s'y conformer. Or l'Assemblée fédérale en a décidé autrement en supprimant ces dispositions transitoires. Cela signifie que les nouvelles obligations de la nLPD seront opposables à tout responsable du traitement dès l'entrée en vigueur de la loi, et ce sans délai de transition. Au vu de ce qui précède, les responsables du traitement seraient bien avertis de d'ores et déjà réfléchir à leur mise en conformité avec la nLPD.

Subsiste une exception prévue à l'art. 69 nLPD s'agissant des dispositions relatives aux nouveaux principes de protection des données dès la conception et par défaut (art. 7 nLPD) et aux obligations de réaliser une analyse d'impact relative à la protection des données (art. 22 et 23 nLPD). Ces dispositions ne s'appliquent pas, à la triple condition que:

a) les traitements aient débuté avant l'entrée en vigueur de la nLPD et pour autant que

b) les finalités du traitement restent inchangées et que  
c) de nouvelles données personnelles ne soient pas collectées.

**2.2 Ce qui ne changera (presque) pas.** La nLPD régit tout traitement de données personnelles concernant une personne physique effectué par des personnes privées ou par des organes fédéraux (art. 2, al. 1, let. a et b, nLPD). Le champ d'application à raison de la matière et de la personne reste donc presque inchangé, à l'exception du fait que les personnes morales ne sont plus comprises dans celui-ci. Ces dernières continuent toutefois de bénéficier de la protection du code civil suisse. Quant au champ d'application territorial, celui-ci est désormais explicitement mentionné à l'art. 3 nLPD.

Les principes généraux de la protection des données (art. 6 et 7 nLPD) restent inchangés, à une exception près avec le principe de transparence qui devra notamment se traduire par un devoir d'information accru (art. 19 et 20 nLPD). En outre, deux nouveaux principes sont intégrés. Il s'agit premièrement du principe de protection des données dès la conception (art. 7, al. 1 et 2, nLPD) qui oblige le responsable du traitement à concevoir, dès l'origine, le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. Ensuite, le principe de la protection des données par défaut (art. 7, al. 3, nLPD) impose au responsable de traitement de garantir que le traitement de données personnelles soit limité au minimum requis par la finalité poursuivie, notamment par le biais de préférences appropriées [14].

Le concept suisse selon lequel le traitement de données personnelles, dans le secteur privé, est en principe autorisé sous réserve d'une atteinte à la personne (art. 30 nLPD) reste le même. De ce point de vue, la nLPD s'éloigne donc du RGPD, lequel interdit le traitement de données personnelles et ne l'autorise qu'en présence d'un motif légal tel que le consentement, l'intérêt légitime ou l'exécution d'un contrat (art. 6 RGPD).

Les motifs pour lesquels les traitements de données personnelles peuvent être justifiés (art. 31 nLPD) restent les mêmes. Des restrictions ont toutefois été ajoutées s'agissant des données personnelles traitées à des fins de recherche, de planification ou de statistique (art. 31, al. 2, let. e, nLPD) et pour l'évaluation de la solvabilité (art. 31, al. 2, let. c, nLPD). Dans ce dernier cas, les entreprises évaluant la solvabilité ne doivent pas garder des données vieilles de plus de dix ans.

S'agissant de la validité du consentement, la nLPD n'est pas différente de la loi actuelle, sous réserve de l'ajout du consentement exprès en cas de profilage à risque élevé. En particulier, la nLPD ne va pas aussi loin que le droit européen en ce qui concerne les conditions applicables au consentement (art. 7 RGPD). Il n'est par exemple pas nécessaire d'informer une personne sur la possibilité de retrait du consentement et un consentement donné de manière générale, servant ainsi plusieurs finalités, reste possible (art. 6, al. 6, nLPD *a fortiori*).

Enfin, les pouvoirs du Préposé fédéral à la protection des données et à la transparence (PF PDT) seront renforcés. En effet, le PF PDT aura le pouvoir d'émettre de réelles injonc-

tions et non pas de simples recommandations (art. 51 nLPD). Toutefois, il ne sera pas habilité à prononcer des amendes administratives, à l'instar de ses homologues européens ou encore de la Commission de la concurrence. La sanction pénale en lien avec la violation des obligations d'informer, de renseigner et de collaborer (art. 60 nLPD) ou des devoirs de diligence (art. 61 nLPD) sera une amende de CHF 250 000 au plus, ce qui est extrêmement modeste par rapport à ce que permet le RGPD.

## 2.3 Ce qui changera

**2.3.1 Devoir d'informer lors de la collecte de données personnelles et exceptions (art. 19–20 nLPD).** L'obligation de fournir des informations lors de la collecte de données personnelles a été étendue dans le cadre de la nLPD, mais elle l'est moins qu'en droit européen (art. 12 à 14 RGPD). Le responsable du traitement devra fournir à la personne concernée l'identité et les coordonnées du responsable du traitement, la finalité du traitement et, le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises. Afin de s'assurer que les personnes concernées puissent effectivement prendre connaissance des informations nécessaires, celles-ci pourraient être transmises par le biais de conditions générales incorporées au contrat ou par une page web dédiée à la protection des données [15].

Par ailleurs, l'art. 19, al. 4, nLPD obligera également le responsable du traitement à informer la personne concernée, en cas de communication des données à l'étranger (p. ex. dans le cadre d'un recours à un hébergement «cloud» dont les serveurs seraient basés hors de Suisse), du nom de l'État ou de l'organisme international auquel les données sont communiquées. Selon nous, il sera nécessaire de communiquer précisément le nom de l'État dans lequel les données seront communiquées [16]. En effet, la simple mention d'une zone géographique à l'instar de «l'Amérique du Nord» ne sera pas suffisante au regard du libellé clair de la loi. En outre, si le responsable du traitement privé a son siège à l'étranger, il devra également désigner un représentant en Suisse et communiquer son nom (art. 14, al. 3, nLPD) [17].

**2.3.2 Sous-traitance (art. 9 nLPD).** Dans le cas d'un traitement de données, il arrive que le responsable du traitement fasse appel à un sous-traitant. Ce dernier ne traite pas les données pour son propre compte, mais pour le compte du responsable du traitement et sur ses instructions. Il s'agit donc d'un acteur possible, mais non nécessaire [18].

Actuellement, la sous-traitance implique certaines exigences formelles, en particulier l'existence d'un contrat (art. 10 a LPD). La nLPD a toutefois apporté une modification au régime actuel. Le responsable du traitement devra préalablement autoriser son sous-traitant à recourir lui-même à un (sous-)sous-traitant (art. 9, al. 3, nLPD). L'autorisation ne sera soumise à aucune exigence de forme, mais le responsable du traitement devra pouvoir prouver à tout moment cette autorisation, si bien qu'il sera dans son intérêt de la documenter [19]. Dans l'hypothèse où des données personnelles sous-traitées seraient transférées à l'étranger, le responsable du traitement devrait encore veiller aux condi-

tions liées à la communication de données personnelles à l'étranger [20].

En comparaison, l'art. 28 RGPD est plus exigeant d'un point de vue formel, notamment en lien avec un certain nombre d'éléments dans le contrat de sous-traitance. Au vu de la généralisation dans le domaine de la protection des données à recourir à des contrats de type RGPD, la conformité devrait être assez aisée pour les responsables du traitement. À l'avenir, le responsable du traitement devra tout de même s'assurer que les clauses du contrat de sous-traitance font référence à la fois aux exigences prescrites par la nLPD que par le RGPD.

**2.3.3 Conseiller à la protection des données (art. 10 nLPD).** Le conseiller à la protection des données est la personne, au sein d'une entreprise, chargée de veiller au respect des prescriptions de protection des données et de prodiguer des conseils en la matière [21]. Contrairement à l'art. 37 RGPD qui prévoit, dans certains cas, une obligation de nommer un tel conseiller, l'art. 10 nLPD ne fait que mentionner cette possibilité, sans pour autant rendre cette institution obligatoire. Ceci est regrettable tant le conseiller à la protection des données est essentiel à la bonne gouvernance d'une entreprise en matière de protection des données et dans la gestion de son patrimoine informationnel.

**2.3.4 Registre des activités de traitement (art. 12 nLPD).** Actuellement, le responsable du traitement qui traite des données sensibles ou des profils de la personnalité doit tenir un registre des fichiers (art. 11a LPD) qui est publié [22]. Avec le nouveau droit, chaque responsable du traitement et sous-traitant devra tenir un registre de ses activités de traitement (art. 12, al. 1, nLPD). Des exceptions seront toutefois prévues au sein de la future ordonnance fédérale à la double condition que l'entreprise emploie moins de 250 collaborateurs et que le traitement ne présente qu'un risque limité. Cette nouvelle obligation peut représenter un travail important pour le responsable du traitement privé n'étant actuellement pas tenu de déclarer ses fichiers.

Comparable au registre des activités de traitement prévu à l'art. 32 RGPD, les indications minimales à faire figurer dans le registre se trouvent à l'art. 12, al. 2, nLPD. Toutefois le registre des activités de traitement d'un responsable du traitement privé n'aura pas à être publié (art. 56 nLPD *a contrario*), contrairement à la solution retenue dans le droit actuel.

Outre les informations minimales à faire figurer au sein du registre, nous conseillons au responsable du traitement d'intégrer d'autres informations, comme le nombre de personnes concernées par le traitement, la durée de conservation des données, le lieu de stockage des données et de ses sauvegardes, les processus internes liés à l'accès aux données personnelles ainsi que les mécanismes de contrôle mis en place [23].

La Commission nationale de l'informatique et des libertés (CNIL), soit l'autorité française de protection des données, met à disposition sur son site web des modèles de registre en français, certes fondés sur le RGPD, mais dont il est possible de s'inspirer [24].



2.3.5 *Communication de données personnelles à l'étranger (art. 16–17 nLPD)*. La nLPD continuera de régir les transferts transfrontaliers de données personnelles, mais de manière légèrement différente. Tout d'abord, il n'appartiendra plus au PFPDT de déterminer les pays considérés comme ayant une législation assurant un niveau de protection adéquat. En effet, cette charge sera dévolue au Conseil fédéral (art. 16, al. 1, nLPD)[25]. En dépit de l'absence d'une telle législation, le transfert de données personnelles restera possible aux conditions imposées par l'art. 19, al. 2, nLPD et, éventuellement, par d'autres conditions qui doivent être définies dans l'ordonnance (art. 19, al. 3, nLPD). À cet égard, les clauses contractuelles types de l'Union européenne pourront continuer à être utilisées avec la nLPD.

2.3.6 *Représentant (art. 14–15 nLPD)*. Conformément à l'art. 14 nLPD, le responsable du traitement privé qui a son siège ou son domicile à l'étranger devra désigner un représentant en Suisse aux trois conditions cumulatives suivantes:

- a) le traitement est en rapport avec l'offre de biens ou de services ou le suivi du comportement de personnes en Suisse;
- b) il s'agit d'un traitement à grande échelle et régulier; et
- c) il présente un risque élevé [26] pour la personnalité des personnes concernées [27].

Le nom du représentant, ainsi que son adresse, devront en outre être publiés. Enfin, le représentant devra tenir un registre des activités de traitement (art. 15, al. 1, nLPD).

2.3.7 *Analyse d'impact relative à la protection des données personnelles (art. 22–23 nLPD)*. Lorsque le traitement de données envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement devra, au préalable, procéder à une analyse d'impact relative à la protection des données (art. 22, al. 1, nLPD).

Bien que floue, la notion de «risque élevé» [28] a été introduite au sein de diverses dispositions légales de la nLPD (art. 5, let. g; art. 14, al. 1, let. d; art. 22 et 23; art. 24). Concrètement, l'évaluation du risque devra être opérée en relation avec la vraisemblance qu'il se réalise et avec la gravité qu'il représente pour les personnes concernées. Le risque devra également être examiné en relation avec son étendue, en tenant compte de la nature des données collectées, de leur volume, de leur variété, de leur sensibilité, de la durée de l'opération de traitement ou encore de la zone géographique.

À titre d'exemple, le Comité européen de la protection des données (CEPD) a précisé, dans ses lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contact dans le cadre de la pandémie de COVID-19, qu'une analyse d'impact devait être effectuée avant la mise en œuvre d'outils de traçage dans le contexte de la pandémie qui secoue le monde entier [29]. Quand bien

même la Suisse n'est pas soumise à ces lignes directrices et que l'obligation de réaliser une analyse d'impact n'est pas encore en vigueur, le projet de traçage DP-3T, développé notamment par les écoles polytechniques de Lausanne et de Zurich [30], a fait l'objet d'une telle analyse d'impact qui a été publiée [31]. Même si la publication de cette analyse n'était pas une obligation sous l'angle du droit en vigueur et ne le sera pas non plus dans la nLPD, cela a assurément contribué à renforcer la transparence du traitement et la confiance dans un tel outil.

2.3.8 *Annonce des violations de la sécurité des données (art. 24 nLPD)*. Conformément à l'art. 24 nLPD, le responsable du traitement devra annoncer au PFPDT dans les meilleurs délais les cas de violation de la sécurité des données entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. La notion de violation de la sécurité des données est définie à l'art. 5, let. h, nLPD comme étant «toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données».

L'obligation d'annonce dépendra essentiellement du seuil de gravité de la violation, qui devra, selon la nLPD, entraîner un «risque élevé». Nous pouvons notamment penser ici au cas de la cyberattaque entraînant la copie de données personnelles pouvant conduire à une usurpation d'identité, une perte réputationnelle ou financière.

En comparaison, le RGPD est plus sévère, puisque doit être annoncée toute faille engendrant un «risque» (art. 33 RGPD), sans qu'il y ait d'exigence de gravité.

### 3. CONCLUSION

L'adoption de la nLPD permet la ratification par la Suisse de la Convention 108 modernisée. Dans le même temps, la Commission européenne devra évaluer, en vertu de l'art. 97 RGPD, notre nouvelle législation afin de nous accorder, ou non, l'adéquation facilitant la communication de données personnelles transfrontalières. Les cantons ne sont pas en reste, puisqu'ils devront également adapter leur législation cantonale en matière de protection des données pour se conformer aux acquis Schengen.

Cette nouvelle loi ouvre aussi un nouveau chapitre pour les entreprises traitant des données en Suisse ou visant le marché suisse. En effet, de nouvelles obligations incomberont aux responsables du traitement et il y aura lieu de les respecter dès l'entrée en vigueur de la nLPD. Il y a deux ans, le RGPD a défrayé l'actualité européenne et suisse en raison notamment de la crainte provoquée par le montant des amendes administratives que cet instrument permet de prononcer. Si la nLPD n'a pas fait l'objet d'autant de discussions sur ce point, tout responsable du traitement privé serait bien mal avisé de ne pas se mettre en conformité d'ici l'entrée en vigueur. ■

**Notes:** **1)** Une chronologie plus détaillée est accessible à l'adresse suivante: <https://swissprivacy.law/11/> (consulté le 24 octobre 2020). **2)** Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données du 9 décembre 2011 (cité: FF 2015, 255–272). **3)** FF 2015, p. 267–268 (note 2). **4)** Rapport du groupe d'accompagnement – Esquisse d'acte normatif relative à la révision de la LPD du 29 octobre 2014. Le rapport est accessible à l'adresse suivante: <https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf.download.pdf/ber-normkonzept-f.pdf> (consulté le 24 octobre 2020). **5)** Il s'agissait ici des réformes législatives en lien avec le Règlement général sur la protection des données (RGPD), qui a remplacé la Directive 95/46/CE. Outre l'encre qu'il a fait couler dans la littérature juridique, notamment en lien avec son champ d'application extraterritorial, nous rappelons que le règlement est entré en vigueur le 24 mai 2016 et qu'il est entièrement applicable depuis le 25 mai 2018. Contrairement à la nLPD, une période transitoire de deux ans était laissée aux responsables du traitement pour adapter leur traitement de données personnelles. **6)** Le Conseil de l'Europe travaillait alors sur la modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. **7)** L'avant-projet est accessible à l'adresse suivante: <https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vorentw-f.pdf.download.pdf/vorentw-f.pdf> (consulté le 24 octobre 2020). **8)** Rapport explicatif concernant

l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016. Le rapport est accessible à l'adresse suivante: <https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-f.pdf.download.pdf/vn-ber-f.pdf> (consulté le 24 octobre 2020). **9)** Synthèse des résultats de la procédure de consultation de l'avant-projet de LPD du 10 août 2017. La synthèse est consultable à l'adresse suivante: <https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-f.pdf.download.pdf/ve-ber-f.pdf> (consulté le 24 octobre 2020). **10)** Projet LPD (FF 2017, 6803–6884). **11)** Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017, 6565–6802; cité: Message LPD 2017, FF 2017). **12)** Objet 17.059 Loi sur la protection des données. Révision totale et modification d'autres lois fédérales. **13)** FF 2020, 7397–7488. **14)** Message LPD 2017, FF 2017 p. 6648–6649 (note 11). **15)** Avec par exemple une politique de confidentialité, une politique de protection des données, une privacy notice. **16)** Si les données transitent par plusieurs États, ceux-ci devront être listés. **17)** Cf. infra 2.3.6. **18)** Il sied de rappeler que ne sont pas constitutifs de cas de sous-traitance les traitements de données au sein d'une même personne juridique (Message LPD 2017, FF 6565, p. 6652 [note 11]). **19)** Message LPD 2017, FF 6565 p. 6651 (note 11). **20)** Cf. infra 2.3.5. **21)** Message LPD 2017, FF 6565 p. 6652 (note 11). **22)** Le registre des fichiers est publié à l'adresse sui-

vante: [www.datareg.admin.ch](http://www.datareg.admin.ch) (consulté le 24 octobre 2020). **23)** Un tel ajout au sein de son registre des activités de traitement permet également au responsable du traitement d'anticiper les informations à transmettre à une personne exerçant son droit d'accès conformément à l'article 25 nLPD. **24)** Les modèles sont accessibles à l'adresse suivante: <https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement> (consulté le 24 octobre 2020). **25)** La liste actuelle est accessible à l'adresse suivante: [https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/04/staatenliste.pdf.download.pdf/liste\\_des\\_etats.pdf](https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/04/staatenliste.pdf.download.pdf/liste_des_etats.pdf) (consulté le 24 octobre 2020). **26)** Sur cette notion, voir infra 2.3.7. **27)** Sur ce dernier point, voir infra 2.3.7. **28)** Cette notion soulève plusieurs questions que nous avons déjà examinées dans une contribution auquel nous renvoyons le lecteur: Livio di Tria, L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, in: *sic! 3/2020*. **29)** À cet égard, voir le § 38 des lignes directrices mentionnées. Celles-ci sont accessibles à l'adresse suivante: [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_20200420\\_contact\\_tracing\\_covid\\_with\\_annex\\_fr.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf) (consulté le 24 octobre 2020). **30)** Système de traçage utilisé par l'application SwissCovid. **31)** L'analyse d'impact est disponible à l'adresse suivante: [https://github.com/DP-3T/documents/blob/master/data\\_protection/DP-3T%20Model%20DPIA.pdf](https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf) (consulté le 24 octobre 2020).