28e Rapport d'activités 2020/21

Préposé fédéral à la protection des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2020/2021
du Préposé fédéral à la protection des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence est tenu de fournir périodiquement à l'Assemblée fédérale un rapport sur son activité (art. 30 LPD).

Le présent rapport couvre la période du 1er avril 2020 au 31 mars 2021.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Avant-propos

L'année sous revue a été marquée par une pandémie persistante et par les mesures que le Conseil fédéral et son administration ont prises afin de protéger la population et de soutenir l'économie.

Dans ce contexte, notre autorité a naturellement concentré son activité de surveillance sur les supports numériques de lutte contre la pandémie tels que l'application SwissCovid ou le certificat sanitaire. Le coronavirus a également marqué notre quotidien dans l'application de la loi sur la transparence car une part importante des demandes en médiation qui nous sont parvenues portaient sur l'accès à des documents officiels relatifs, par exemple, à l'achat de masques ou de vaccins.

Alors que l'État, aux prises avec la pandémie, est intervenu dans la sphère privée et dans l'autodétermination informationnelle de la population par une série de mesures mises en oeuvre à un rythme rapide, notre équipe a revendiqué la transparence de l'action des autorités. Comme l'administration est obligée, en temps de crise, de définir des priorités, nous avons procédé avec pragmatisme en demandant par exemple aux journalistes de faire preuve de patience concernant la documentation a posteriori des activités de l'Office fédéral de la santé publique.

Il est trop tôt pour dresser le bilan des dommages causés par cette pandémie liberticide. Mais une chose est sûre : notre autorité a elle aussi tiré les leçons des défaillances numériques qui ont suscité la surprise et l'indignation au cours de cette crise. La critique des services de l'État et des dirigeants ne doit pas pour autant masquer les déficits engendrés par la transformation numérique asynchrone de notre pays, à commencer par le défaut d'identité électronique officielle, un service de base qui se révèle indispensable à une gestion moderne et sûre des données de santé.

Adrian Lobsiger
Préposé fédéral à la protection des données et à la transparence

Berne, le 31 mars 2021

Protection des données

Textes et images avec référence Corona

Défis actuels

I Numérisation

La crise du coronavirus, qui perdure malgré les vaccins, et son effet accélérateur sur la transformation numérique des modes de travail et de consommation ont encore marqué, pendant l'année sous revue, le rapport de la population suisse aux technologies de l'information et de la communication.

Technologie et économie

La sphère privée et les droits à l'autodétermination des citoyens restent très vulnérables face au pouvoir d'intrusion de la technologie et de l'économie.

La réalité numérique repose sur la cybertransmission, à la vitesse de la lumière, de signaux que des milliards d'appareils portables, dits intelligents (« Smart Devices »), transposent en textes, en images, en sons ou en vibrations afin de les rendre perceptibles par les sens. La disponibilité permanente et la large diffusion de ces informations satisfont la curiosité, le goût du jeu et la soif de savoir de notre société.

Mais elles pèsent aux citoyens dès qu'entrent en jeu des exigences particulières concernant l'utilisation des données ou la protection de la sphère privée. Particuliers et entreprises ont ainsi pris l'habitude de cloisonner et de crypter une partie de leurs données, au grand dam de la police et de l'administration restrictive. En même temps, un nombre croissant d'autorités et d'acteurs privés demandent aux détenteurs d'appareils intelligents de présenter leur appareil pour effectuer, au moyen d'une application spéciale, une synchronisation automatique des données, ce qui peut générer une certaine gêne à l'idée que l'on puisse, de ce fait, retracer une partie du comportement numérique de chacun. D'où la réticence de certains à obtempérer. Sans compter les personnes qui, en raison de leur âge, de leur état de santé ou d'un handicap, n'utilisent pas ce genre d'appareil.

Le stade actuel de la lutte contre la pandémie indique que ces personnes vont faire l'objet de pressions croissantes. Dans la perspective de la réouverture des établissements et de la levée des interdictions de se rassembler, il est probable que l'accès à certains biens et services sera prochainement subordonné à la présentation d'un test COVID-19 négatif ou d'un certificat de vaccination. Afin que la détention d'un smartphone ne devienne pas peu à peu une obligation, le PFPDT demande qu'on propose aux citoyens, pour recueillir leurs données de santé, des alternatives raisonnables au tout numérique. C'est d'autant plus important que selon toute vraisemblance, le traitement systématique de données personnelles qui s'est généralisé dans le contexte de la pandémie aura des répercussions sur l'autodétermination informationnelle de la population bien au-delà de la crise actuelle. Les appareils intelligents étant très répandus, il y a lieu de craindre que la crise ne devienne le marchepied d'intérêts étatiques et commerciaux selon lesquels, au prétexte que ces appareils sont accessibles en permanence, il faudrait les utiliser comme moyens d'identification et de documentation. Afin d'éviter que les smartphones ne dégénèrent en entraves numériques, le Préposé a exigé publiquement que des supports d'information courants tels que le papier soient également autorisés pour le recueil des coordonnées dans le cadre du traçage des contacts, de même que pour les résultats de test et pour les certificats de vaccination (cf. nos communications sur la collecte des données destinée au traçage des contacts et celle sur la collecte de données de santé par des acteurs privés). Ce sont probablement des réflexions analogues qui ont incité le législateur fédéral, au début de l'été 2020, à inscrire dans la loi sur les épidémies le principe selon lequel personne ne peut faire dépendre l'obtention d'une prestation de l'utilisation de l'application Swiss Covid.

Au cours de l'année sous revue, l'automatisation croissante du traitement de gros volumes de données a aussi montré l'ampleur de ses effets sur l'organisation des élections et des votations. Lorsque des techniques mécaniques et numériques sont utilisées pour dépouiller un scrutin important, la première inquiétude des électeurs porte sur la transparence et la fiabilité de ces techniques, et donc sur la protection des données.

Cette méfiance largement répandue a contribué aux troubles qui ont suivi la dernière élection présidentielle américaine. Par leur critique générale du système, axée plus particulièrement sur les aspects techniques abstraits de la transmission, du comptage et de l'évaluation des données, les avocats de la Maison-Blanche de l'époque ont renforcé les doutes d'un public exposé, sur les forums du web, à un feu nourri de raisonnements complotistes dénonçant, entre autres «manigances», des algorithmes biaisés. Compte tenu de ces éléments, on peut s'attendre à ce que l'automatisation croissante des élections et des votations renforcera, parmi les outils du droit moderne de la protection des données, l'importance de ceux qui nécessitent un minimum d'interventions humaines dans les procédures menant à des décisions.

Société et politique des données

Le 7 mars 2021, le peuple suisse a rejeté massivement le projet de loi fédérale sur les services d'identification électronique (e-ID). Tandis que le Conseil fédéral et le Parlement appelaient en vain les citoyens à accorder leur confiance à une e-ID émise par des entreprises privées, le comité référendaire a convaincu par son argument clé, qui était que l'émission de pièces d'identité doit rester une responsabilité de l'État. Si le peuple revendique une intervention accrue de l'État dans un projet numérique clé, c'est sans doute parce qu'il s'attend légitimement à ce que, d'une part, l'action de l'État et le traitement de données personnelles qui en découle se limitent à ce que prévoit la loi, et d'autre part, que les autorités appliquent le principe de légalité.

Ces attentes présentent un certain décalage par rapport à l'expérience du PFPDT. Dans le cadre de son activité de conseil et de surveillance, le Préposé constate en effet que l'administration, confrontée au défi de la transformation numérique, se montre de plus en plus rétive au principe de légalité et met en doute les exigences que la pratique des tribunaux fédéraux formule quant à la fermeté des bases légales du traitement de données personnelles. Selon le Préposé, l'administration estime par exemple que plus rien ne justifie de préciser dans la loi le contenu, les catégories, les finalités, l'intensité et la durée du traitement de données par les autorités, au motif que cela implique la conservation de « silos » de données archaïques et des «ruptures de support» qui empêchent l'administration d'interagir avec souplesse et de travailler efficacement.

Le Préposé, lui, non seulement ne remet pas en cause la transformation numérique de l'administration fédérale, mais il insiste aussi sur la nécessité de créer des bases légales modernes, qui n'entravent pas inutilement la liberté d'action des offices sur le plan de l'organisation et de la technologie. En prodiguant des conseils axés sur les solutions, il prouve que les prescriptions légales de portée générale et technologiquement neutres ne nuisent en rien à la transformation numérique. Il soutient aussi les efforts de l'administration pour simplifier les structures héritées du passé.

Cette ouverture au progrès ne lui permet pas pour autant de dispenser l'administration de fonder le but, l'ampleur et l'intensité du traitement

«La détention d'un smartphone sur soi ne doit pas devenir une obligation pour la population»

numérique des données personnelles sur un mandat des organes politiques inscrit dans la loi d'une manière compréhensible pour les citoyens. Il est par ailleurs indispensable que le législateur, qui jouit de la légitimité démocratique, fixe, lorsqu'il réglemente le traitement de données par les autorités, des limites de compétence eu égard à la politique et à l'état de droit, en attribuant des responsabilités, en restreignant l'accès direct aux données personnelles et en réglementant les échanges d'informations par la voie de l'assistance administrative. La nécessité de concilier la transformation numérique de l'administration et le principe de la légalité découle d'ailleurs de la nouvelle LPD, où le législateur de 2020 a matérialisé la promesse qu'un organe fédéral ne peut traiter des données sensibles de citoyens que si une loi soumise au référendum le prévoit et précise la finalité, l'ampleur et l'intensité du traitement de même que la nature et le contenu des données.

Au cours de la période sous revue, le Préposé a débattu des exigences du principe de légalité avec l'Administration fédérale des douanes, notamment. Il s'agissait en l'occurrence des marges de manœuvre du futur Office fédéral de la douane et de la sécurité des frontières, dont le personnel sera amené à traiter des gros volumes de données sensibles, et de la double question de l'armement et des compétences policières des collaborateurs de l'Office fédéral de la police ou du Service de renseignement de la Confédération.

Le traitement de données personnelles par ces autorités fédérales de sécurité comporte des risques importants pour la sphère privée et pour l'autodétermination informationnelle de la population car ces autorités procèdent secrètement à l'obtention de certaines informations et peuvent, selon le résultat de l'évaluation des données, imposer des mesures coercitives radicales aux personnes concernées. Compte tenu de ces éléments, le PFPDT ne peut tolérer aucune concession concernant le respect des exigences des tribunaux fédéraux quant à la fermeté des bases légales du traitement de données personnelles par les autorités policières. Seules des lois suffisamment fermes permettront d'éviter que la transformation numérique n'amène, chez les autorités fédérales de sécurité et les corps de police cantonaux, une dilution des compétences. Si on permettait aux autorités d'apparier à leur guise les données personnelles qui sont traitées dans le tissu confédéral des autorités de sécurité à des fins aussi diverses que la prévention des dangers (police de sécurité), la poursuite pénale (police judiciaire), la protection de l'État (service de renseignement) ou l'exécution de nombreuses lois spéciales, il en résulterait une concentration opaque de pouvoirs policiers incompatible avec l'organisation des compétences établie par la Constitution fédérale.

Il importe d'autant plus de restreindre, dans la loi, le traitement de données par la police fédérale à des catégories de tâches spécifiques, que l'organisation des autorités de sécurité est, pour des raisons historiques, bien plus complexe à l'échelon de la Confédération qu'à celui des cantons. À l'échelon des cantons, la collecte cachée et forcée de données personnelles incombe à un corps de police unique dont les tâches et les compétences sont définies dans la loi cantonale sur la police, facile à consulter, tandis que la Confédération, on l'a vu, répartit son pouvoir policier entre plusieurs forces armées, qui traitent des données personnelles en vertu de différentes lois fédérales. Le Préposé dénonce depuis de nombreuses années dans son rapport d'activités le fait que l'inexistence d'un acte comparable aux lois cantonales sur la police et que la pléthore de lois spéciales fédérales nuisent, d'une manière peu défendable en vertu de la législation sur la protection des données, à la transparence du traitement de données par les autorités fédérales de sécurité. À l'ère de la transformation numérique, ce morcellement du droit fait que ces autorités ont de plus en plus de mal à garder une vue d'ensemble de leurs multiples traitements de données. Le Préposé voit

«Les autorités fédérales de sécurité ont de plus en plus de mal à respecter le principe de légalité.»

dans ce phénomène une explication supplémentaire à la réticence croissante des autorités de sécurité de la Confédération à appliquer le principe de légalité.

Législation

Les Chambres fédérales ont mené à bien de longs travaux en adoptant, le 25 septembre 2020, la révision totale de la loi fédérale sur la protection des données (cf. Accent I).

II Activités de conseil, de surveillance et de médiation

En tant qu'autorité de surveillance, le Préposé doit veiller à ce qu'indépendamment des possibilités techniques, le traitement de données personnelles soit conforme à la loi. Il exige donc des responsables d'applications numériques qu'ils anticipent et réduisent autant que possible les risques en matière de protection des données dès le stade de la planification et de l'élaboration, et qu'ils les documentent vis-à-vis de leur surveillance interne et des autorités compétentes. Dans cet esprit, il a poursuivi l'accompagnement de nombreux projets d'autorités fédérales et d'entreprises privées impliquant des mégadonnées, en encourageant l'utilisation responsable d'outils modernes tels que l'analyse d'impact en matière de protection des données ou la désignation de responsables de la protection des données dans les entreprises.

Pendant la période sous revue, le Préposé s'est focalisé sur l'accompagnement et le contrôle des nombreux projets numériques liés à la lutte contre la pandémie, qui sont signalés dans le présent rapport par la couleur jaune. La pandémie a aussi suscité pour lui de nombreuses difficultés sur le plan de la transparence. Il s'est ainsi retrouvé confronté à une multitude de demandes en médiation concernant notamment des documents officiels sur l'acquisition de masques ou de vaccins, dont la plupart ont donné lieu, pour cause de télétravail obligatoire, à des recommandations écrites représentant une charge de travail considérable.

Des quinze grands projets que le Préposé a accompagnés dans le cadre de son devoir de conseil, six avaient trait à la transformation numérique de l'administration fédérale ordonnée par le Conseil fédéral afin de rattraper le retard dénoncé par les politiques et les médias et dû notamment à la lutte contre la pandémie. Ces projets émanaient de l'Office fédéral de la santé publique et de nombreux autres organes fédéraux, dont les autorités de sécurité (cf. ci-dessus et ch. 1.2 et 3.1).

Alors que les dépenses affectées aux tâches de surveillance avaient nettement diminué au cours de la période 2015-2016, elles ont réaugmenté légèrement ces dernières années, se stabilisant à un niveau faible en raison de l'insuffisance persistante des moyens. Pendant la période sous revue, le Préposé n'a pas été à même, une fois de plus, de répondre dans la mesure souhaitée aux attentes justifiées du public. Malgré sa volonté de collaborer étroitement avec le Centre national pour la cybersécurité, il manque de moyens (cf. ch. 3.1) pour effectuer systématiquement les vérifications et les contrôles aléatoires de la sécurité technique qu'exigent pourtant les bases de données sensibles sur la santé. Dans ce contexte, il convient de rappeler le cas de la fondation «mesvaccins».

III Coopération nationale et internationale

Coopération nationale

La lutte contre la pandémie de COVID-19 a fait émerger des questions de délimitation des compétences entre la Confédération et les cantons, tant pour le traçage des contacts que pour le traitement de données personnelles liées aux vaccins et aux tests. Grâce aux bonnes relations qui se sont instaurées entre les responsables cantonaux de la protection des données et le PFPDT, les solutions adoptées s'inscrivent toutes dans une logique pragmatique de concertation.

Coopération internationale

Le traitement de données de santé dans le cadre de la lutte contre la pandémie suscite dans bien des pays des questions semblables quant à la protection des données. Le PFPDT a donc suivi attentivement les développements internationaux et mis à profit ses contacts avec ses homologues étrangers.

Conseil de l'Europe

Le PFPDT a à cœur de s'impliquer activement dans le Conseil de l'Europe. Il a donc continué de participer aux séances du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Une représentante du PFPDT a d'ailleurs été nommée au Bureau du Comité consultatif, qui dirige les travaux de celui-ci entre les séances plénières.

Évaluation du niveau de protection des données

Le rapport de la Commission européenne évaluant le niveau de protection des données en Suisse, attendu pour la fin mai 2020, a pris du retard mais devrait arriver avant l'été 2021.

La Suisse a par contre pu mener à bien au cours de l'année sous revue la reconnaissance mutuelle, avec le Royaume-Uni qui a quitté l'UE, de leurs niveaux de protection de données.

Insuffisance du Swiss-US Privacy Shield comme niveau de protection des données

La Cour de justice de l'Union européenne (CJUE) a rendu le 16 juillet 2020 un arrêt très attendu (Schrems II) concernant le transfert de données entre l'UE et les États-Unis. Elle y invalide la décision 2016/1250 de la Commission européenne relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.

Les arrêts de la CJUE ne s'appliquent pas à la Suisse. Toutefois, lors de son évaluation périodique du bouclier de protection des données Suisse-États-Unis (Swiss-US Privacy Shield) et des reconnaissances d'adéquation entre la Suisse et l'UE, le Préposé a constaté que ce régime n'offrait plus aux personnes concernées un niveau de protection approprié en Suisse. Il a par conséquent invité les entreprises suisses à effectuer les transmissions futures de données vers les États-Unis sur la base de garanties contractuelles et d'analyses des risques au cas par cas.

Protection des données

1.1 Numérisation et droits fondamentaux

Analyse d'impact relative à la protection des données concernant SwissID

Au cours de l'année sous revue, SwissSign Group SA a soumis au Préposé son analyse d'impact relative à la protection des données concernant SwissID. Du fait de l'importance systémique du service SwissID de SwissSign Group SA, des réunions régulières ont déjà eu lieu à plusieurs reprises par le passé entre les responsables de l'entreprise et le Préposé, lequel s'est notamment

engagé dans ce cadre pour qu'un accès anonyme soit possible pour les purs services SSO (single sign-on) de SwissID. SwissSign Group SA a repris cette demande dans sa politique de protection des données. Les ajustements nécessaires des conditions générales suivront prochainement.

SwissSign Group SA ayant chargé un conseiller externe à la protection des données d'évaluer l'impact de SwissID sur la protection des données, l'analyse d'impact a été transmise au Préposé au cours de l'année sous revue et analysé par ce dernier. Le Préposé a constaté qu'elle contenait une description détaillée des processus de traitement des données personnelles, une évaluation des risques des mesures concernées concernant les droits fondamentaux, ainsi qu'une présentation des mesures de protection de la personnalité.

Le Préposé a pris note que l'analyse d'impact relative à la protection des données était réputée terminée après évaluation par le responsable et que le traitement des données en relation avec SwissID était jugé admissible au vu des risques et des mesures décrits.

Projet d'authentification unique pour les plateformes numériques des médias suisses

L'Alliance numérique suisse poursuit son projet de mise en place d'un système d'authentification unique pour les portails en ligne de ses membres. Dans le cadre d'un échange, le PFPDT a suggéré plusieurs améliorations.
L'Alliance numérique suisse, qui réunit plusieurs médias, entend proposer aux utilisateurs un système d'authentification unique (single sign-on [SSO]) pour se connecter aux différents sites de ses membres. Le projet avance, et une phase pilote a débuté au printemps 2021. Lors des échanges qui ont eu lieu pendant les présentations préliminaires, le PFPDT a exposé à l'Alliance son point de vue sur les aspects importants du projet quant à la protection des données, en suggérant plusieurs améliorations.

Le projet se poursuit au-delà de la publication du présent rapport. Le PFPDT suivra les travaux de près pour faire en sorte que la solution retenue respecte au mieux la protection de la personnalité.

Les services en nuage dans la stratégie informatique de la Confédération

Le PFPDT a accompagné la définition d'objectifs stratégiques et de garde-fous pour la transformation numérique de l'administration fédérale. Les infrastructures nécessaires doivent notamment garantir un recours sûr aux services en nuage publics (public clouds), en plus de l'utilisation des centres de calcul de l'administration fédérale (private clouds). Le Préposé estime qu'il faut intégrer les exigences relevant du droit de la protection des données dès l'appel d'offres.

La transformation numérique implique l'utilisation d'une multitude d'applications et de services devant allier agilité, souplesse et capacité de développement. Les solutions en nuage, qu'elles soient publiques ou privées, y jouent un rôle majeur puisqu'elles proposent les services et les outils requis en temps réel, chaque utilisateur pouvant aller s'y servir lui-même en fonction de ses besoins (voir l'encadré pour les définitions). L'administration fédérale utilise déjà, d'une manière restreinte, différents types de solutions en nuage facilement extensibles. Un sondage mené auprès des départements et de la Chancellerie fédérale fin 2019 a révélé que les besoins en matière de services en nuage publics étaient voués à augmenter.

Ces services assurent aux unités de l'administration fédérale centrale un accès efficace et quasi instantané à des solutions innovantes, relativement bon marché, et à des technologies dernier cri, leur ouvrant des perspectives dans la fourniture de prestations numériques rapides et agiles. Cela permet, dans les domaines n'exigeant pas de mesures de sécurité renforcées, d'optimiser et d'externaliser des prestations d'exploitation informatiques coûteuses. Il y avait donc lieu de créer dans l'administration fédérale, en plus

des solutions privées existantes, une option stratégique pour l'utilisation de services en nuage publics. Il fallait en outre réfléchir à la nécessité, à l'aménagement et à la faisabilité d'une infrastructure en nuage publique 100 % suisse, le « Swiss Cloud ».

Il se trouve que l'utilisation de solutions publiques accroît la dépendance à l'égard des fournisseurs, qui opèrent généralement à l'échelle mondiale, et ce tant pour la technologie que pour la disponibilité des données et des applications. Comment, dans ces conditions, garantir sa souveraineté sur ses propres données et prévenir les risques de fuites ?

En ce qui concerne ces questions, le Préposé a étoffé les critères d'acquisition de solutions en nuage publiques afin que la protection et la sécurité des données soient garanties d'un bout à l'autre de la chaîne, dès le stade du fournisseur. Il s'est aussi investi dans l'élaboration de consignes relatives à la fiabilité de ces services du point de vue de la sécurité de l'information et de la protection des données. Vu la portée de ce projet, le Préposé a en outre considéré qu'il était indispensable d'exiger des soumissionnaires qu'ils fournissent, dans leur offre, la preuve de certifications spécifiques en la matière.

L'expérience montre qu'il faut inclure les questions relevant du droit de la protection des données à un stade précoce des projets impliquant le traitement de données personnelles. Le Préposé continuera d'accompagner les initiatives relatives à l'informatique en nuage et de vérifier que les consignes et les critères correspondants sont bien respectés.

Services en nuage

Alors qu'auparavant, presque toutes les entreprises disposaient de leur propre centre de données, elles sont aujourd'hui nombreuses à utiliser les services en nuage. L'informatique en nuage (en anglais cloud computing) est la fourniture via Internet de services informatiques (espace de stockage, puissance de calcul, logiciels d'application). Un nuage est donc une infrastructure informatique en ligne vers laquelle sont externalisés des données ou des environnements de systèmes entiers. Les solutions en nuage se différencient en fonction de l'utilisation prévue et du degré d'intégration souhaité.

Parmi les grands avantages du nuage, citons :

- une grande extensibilité du système, c'est-à-dire la possibilité d'augmenter et de diminuer aisément la capacité de stockage et la puissance de calcul selon les besoins ;
- une disponibilité et une sécurité élevées grâce à l'utilisation de technologies de pointe ;
- une sécurité de l'investissement, car l'environnement est entretenu et mis à jour par le prestataire et l'entreprise elle-même n'est pas tenue d'investir massivement dans une infrastructure de serveur.

Utilisation du nuage

Il existe différents modèles de mise en œuvre de services en nuage, en fonction des exigences spécifiques des utilisateurs. Les principaux modèles sont :

- le nuage privé : il est généralement installé dans le centre de données de l'entreprise et n'est exploité que par une seule entreprise. Généralement, il est géré par l'entreprise elle-même, ou si nécessaire par un prestataire externe, et n'est accessible qu'à des groupes de personnes clairement définis. Le nuage privé répond à des exigences strictes en matière de sécurité et de protection des données ; il est donc particulièrement adapté aux données sensibles telles que les informations confidentielles relatives au personnel ou les données confidentielles de l'entreprise ;
- le nuage public : il s'agit de l'offre d'un prestataire librement accessible qui met ses services à la disposition de tous sur Internet. Tous les utilisateurs partagent la même infrastructure. Les systèmes de stockage en ligne bien connus tels que Dropbox ou Google Drive, mais aussi les fournisseurs de messagerie tels que Gmail ou Hotmail, sont généralement basés sur un nuage public ;
- le nuage hybride : il s'agit de la combinaison d'un nuage privé et d'un nuage public. L'utilisateur a accès à un nuage public, auquel est intégré un environnement privé pour les données et applications sensibles. Ce modèle est pertinent pour le stockage des données très sensibles dans un nuage privé, tandis que les données moins sensibles sont externalisées plus facilement et à moindre coût ;
- le nuage communautaire : ce modèle connecte plusieurs services en nuage, ce qui implique que les solutions de différents prestataires de nuage peuvent être utilisées en parallèle. Il offre beaucoup plus de possibilités que le nuage hybride.

Profondeur d'intégration du nuage

L'informatique en nuage distingue généralement trois niveaux de services en nuage, prenant appui l'un sur l'autre. De l'infrastructure au logiciel, en passant par la plateforme, ces trois niveaux de service présentent trois couches superposées et constituent en même temps l'architecture en nuage :

- le niveau infrastructure en tant que service (Infrastructure-as-a-Service, IaaS) : les ressources telles que la puissance de calcul, la capacité de stockage ou la capacité de réseau sont disponibles à partir du nuage. Non seulement les serveurs locaux ont été précédemment transférés dans le nuage, mais ce dernier remplace aussi désormais le matériel informatique in situ, tandis que la gestion du système d'exploitation et des applications demeure dans l'entreprise ;
- le niveau plateforme en tant que service (Plattform-as-a-Service, Paas) : dans ce cas, le système d'exploitation et les applications liées au système telles que les applications de sauvegarde, d'antivirus et de maintenance, etc. sont également utilisées à partir du nuage. Au lieu de développer des logiciels sur leur propre environnement, les entreprises peuvent utiliser des environnements complets de développement et de déploiement dans le nuage ;
- le niveau logiciel en tant que service (Software-as-a-Service, SaaS) : l'utilisateur dispose d'une application en nuage avec toutes ses infrastructures et plateformes informatiques fondamentales. Il accède ainsi à tous les composants informatiques auprès du prestataire.

L'entrée de l'administration fédérale dans l'informatique en nuage doit se faire dans le respect de la protection des données

La stratégie d'informatique en nuage de l'administration fédérale vise à ouvrir la voie à une numérisation de l'administration fédérale basée sur l'informatique en nuage. Le Préposé a pris position sur le document de stratégie et a pu faire valoir avec succès ses principales préoccupations du point de vue de la protection des données.

L'Unité de pilotage informatique de la Confédération (UPIC) a été chargée par le Conseil fédéral d'élaborer un document de stratégie concrétisant la vision de la Confédération en matière d'informatique en nuage ; ce document doit aussi prescrire les principes et orientations contraignantes pour l'acquisition d'applications d'informatique en nuage par les différentes unités administratives. Ayant reçu une version préliminaire de ce document en consultation préalable, le Préposé a constaté un potentiel d'amélioration sur différents points. Il a notamment relevé que ce document mettait fortement l'accent sur les exigences en matière de sécurité de l'information, mais n'abordait que superficiellement les autres aspects juridiques de la protection des données.

En conséquence, nous avons proposé des compléments afin d'inscrire dans le document de stratégie les exigences de la protection des données concernant l'externalisation du traitement des données vers un nuage. Nos propositions visaient en particulier à garantir la prise en compte des risques supplémentaires liés à l'externalisation des traitements de données vers des prestataires étrangers de nuage public provenant d'un pays ne disposant pas d'un niveau adéquat de protection des données.

Dans cette optique, afin d'évaluer si le traitement de données sur la base de systèmes informatiques en nuage est autorisé et, dans l'affirmative, de quelles mesures il doit être assorti,

nous avons proposé que le document prévoie la réalisation d'une analyse d'impact relative à la protection des données lorsque des données personnelles sont traitées dans le nuage. Ce mécanisme doit permettre de vérifier la conformité juridique de l'application en nuage, en prenant comme critères la localisation des serveurs, la loi applicable dans le pays en question et les mesures techniques et organisationnelles envisagées. Nos commentaires et les modifications proposées ont été intégrés dans la version finale du document.

L'administration fédérale et les utilisateurs privés de solutions informatiques en nuage publiques sont de plus en plus souvent confrontés à cette question depuis que le bouclier de protection des données Suisse-États-Unis a été réévalué (à propos du bouclier de protection, cf. Accent II du présent rapport) et qu'il ne peut être simplement présumé que les clauses contractuelles types (CCT) garantissent aux États-Unis un niveau adéquat de protection des données. Cela du fait que de nombreux prestataires sont basés aux États-Unis.

CORONA

Accès de l'Office fédéral de la santé publique aux données de mobilité de Swisscom

Le Conseil fédéral ayant interdit les rassemblements de plus de cinq personnes dans l'espace public le 21 mars 2020, l'OFSP a utilisé des informations fournies par Swisscom pour vérifier si cette mesure de protection contre les infections par le coronavirus était respectée. Selon les conclusions du Préposé, Swisscom n'a accordé à l'OFSP qu'un accès à des données anonymisées.

À partir de sa plateforme Mobility Insights (MIP), Swisscom traite des statistiques de groupe anonymisées sur la base de données de mobilité agrégées afin d'évaluer les comportements de mobilité sur le territoire suisse. Ayant appris que l'Office fédéral de la santé publique (OFSP) allait avoir accès à ces données dans le cadre de la lutte contre la pandémie dans le but de vérifier si des personnes se rassemblaient encore en grand nombre en Suisse, le Préposé a engagé des examens préliminaires à ce sujet, dans le cadre desquels il a également procédé à une évaluation de la situation sur place, auprès de l'OFSP.

Les évaluations visualisées rendues accessibles avec un décalage d'au moins huit heures montrent comment la présence de détenteurs de téléphones portables évolue dans le temps, dans un espace de 100 mètres sur 100, si plus de 20 appareils associés à un abonnement Swisscom sont présents dans cet espace. Les données de localisation en question sont dès que possible anonymisées, puis agrégées et l'OFSP ne reçoit à aucun moment les données en clair sur lesquelles se base les visualisations. Les visualisations auxquelles l'OFSP a accès ne permettent d'établir aucun lien avec des personnes spécifiques et sont de ce fait anonymes. En conséquence, dans sa brève évaluation du 3 avril 2020, le Préposé a conclu que le traitement des données opéré par Swisscom et le transfert de données anonymes à l'OFSP respectent le droit de la protection des données (cf. notre communication « L'accès de l'OFSP aux données visualisées de Swisscom est conforme au droit de la protection des données »).

Sur la base de ces informations, le Préposé a décidé de ne pas ouvrir de procédure formelle d'établissement des faits. Il a toutefois estimé que les informations accessibles au public sur la collaboration entre l'OFSP et Swisscom et sur les traitements de données qui y sont associés étaient rares et difficiles à trouver. Il a donc invité Swisscom à publier des informations plus détaillées à propos de ces traitements de données. Swisscom a répondu à cette demande et élaboré des FAQ concernant l'utilisation de la plateforme Mobility Insights de Swisscom par l'OFSP.

Programme de gestion nationale des données

La gestion des données des pouvoirs publics doit être rendue plus simple et plus efficace par l'utilisation multiple des données. Le Conseil fédéral a lancé plusieurs projets pilotes dans ce sens, au titre du Programme de gestion nationale des données. Le Préposé reste en contact avec l'Office fédéral de la statistique, responsable de ces projets, et œuvre en faveur de leur réalisation dans le respect des exigences en matière de protection des données.

Le Programme de gestion nationale des données (NaDB) a pour objectif de décharger les personnes et les entreprises qui ne devront fournir qu'une seule fois certaines informations aux autorités (principe de collecte unique des données, en anglais the Once-Only Principle). De plus, facilitant l'échange de données entre les autorités, l'utilisation multiple des données permettra de réduire la charge administrative de la gestion publique.

En premier lieu, dans le cadre de la consultation des offices, le Préposé s'est prononcé sur les rapports consacrés aux quatre projets pilotes dont les thèmes étaient : l'assurance qualité des données des entreprises, les statistiques des salaires, les données fiscales, ainsi que les processus, rôles et compétences. Il a souligné l'importance cruciale de la protection des données dans l'utilisation multiple des informations que prévoit le programme NaDB. Selon lui, cette utilisation multiple comporte des risques considérables d'atteinte au droit de la protection des données. Il convient notamment de s'assurer que le principe de collecte unique des données ne conduise pas à un élargissement du cercle des utilisateurs habilités. De plus, il est impératif de réglementer qui peut traiter quelles données et à quelle fin. Par ailleurs, une distinction claire doit être faite entre les traitements de données à des fins statistiques et les traitements de données à d'autres fins. Enfin, la collecte des données, le traitement ultérieur de ces données et les possibilités d'accès devront être réglementés de manière transparente.

À la suite de cette procédure de consultation, des échanges ont eu lieu entre le Préposé et l'Office fédéral de la statistique en charge de la réalisation des projets, échanges au cours desquels ces thèmes ont été à nouveau abordés. Le Préposé continuera à accompagner la mise en œuvre du programme NaDB à titre consultatif et restera à la disposition des autorités responsables en tant que personne de contact.

CORONA

Feuillet thématique sur les mesures de sécurité applicables aux conférences audio et vidéo

La pandémie a permis aux applications de conférences audio et vidéo de s'imposer très rapidement dans tous les milieux. Le nombre important de leurs utilisateurs a fait de ces plateformes numériques des cibles intéressantes pour les pirates du web. Lors du choix d'un logiciel, il faut donc veiller tout particulièrement à la sécurité des informations et à la protection des données afin notamment de se prémunir contre un traitement frauduleux de celles-ci et d'éviter les plateformes présentant des faiblesses connues.

Le feuillet thématique du PFPDT (voir notre communication « Mesures de sécurité pour les conférences audio et vidéo » s'adresse à tous les groupes d'utilisateurs, tant professionnels que privés, qui souhaitent protéger leurs données personnelles et éviter les mauvaises surprises. Il recommande un certain nombre de mesures de protection pendant l'utilisation (gestion des identifiants et des mots de passe, utilisation de la caméra et options d'affichage, p. ex.). Il donne aussi des conseils pour évaluer les différentes solutions et pour les mettre en œuvre. Mieux vaut, par exemple, se renseigner sur l'utilisation qui sera faite des métadonnées, sur les méthodes de cryptage et sur la sécurité du fournisseur. Une entreprise aura quant à elle intérêt, avant de généraliser l'emploi d'une application, à édicter un règlement d'utilisation. Elle devra d'ailleurs prévenir ses collaborateurs en toute transparence si elle enregistre ou si elle surveille les réunions.

La tentation étant forte d'intégrer dans l'infrastructure informatique existante les solutions adoptées dans l'urgence pendant la pandémie, le Préposé recommande que l'acquisition des applications fasse l'objet d'un projet ordinaire ou soit confiée aux responsables informatiques, afin de garantir la conformité de l'opération. La solution retenue doit offrir des paramètres de sécurité permettant une protection supérieure des données, notamment en ce qui concerne les secrets professionnel et commercial.

Les traitements de données des applications de rencontre

Le Préposé a ouvert une procédure auprès d'un fournisseur suisse d'applications de rencontre afin d'examiner ses méthodes de traitement et sa gestion des demandes d'effacement.

Selon l'Office fédéral de la statistique, les applications et sites de rencontre jouent en Suisse un rôle de plus en plus important dans le mode de rencontre de là ou du partenaire : près de 20 % des couples dont la relation a commencé au cours des cinq dernières années se sont rencontrés en ligne sur un site de rencontre, via une application de rencontre ou un réseau social[1]. Les sites et les applications de rencontre se caractérisent par le fait qu'ils mettent en relation des partenaires appropriés sur la base des données personnelles des clientes et clients, données qu'ils traitent partiellement ou totalement de manière automatique à l'aide d'un algorithme.

Afin d'augmenter les chances de succès de la recherche de partenaire, les utilisateurs sont invités à révéler des informations parfois très sensibles sur eux-mêmes : données sur leur vision du monde, leur religion, leur consommation d'alcool entre autres. Le traitement de ces données personnelles comporte donc des risques élevés, car elles permettent de tirer des

[1] Office fédéral de la statistique (Éd.) : Enquête sur les familles et les générations 2018. Premiers résultats. Neuchâtel 2019, p. 9. https://www.bfs.admin.ch/bfs/fr/home/statistiques/population/enquetes/efg.assetdetail.10467789.html

conclusions sur des aspects essentiels de la personnalité des utilisatrices et utilisateurs.

Au printemps 2021, le Préposé a ouvert une procédure d'établissement des faits auprès d'un fournisseur, basé en Suisse, offrant ce type d'application de rencontre. Cette procédure fait suite aux annonces qui nous ont été transmises par des personnes dans

l'impossibilité de supprimer leur compte à partir de l'application et dont les demandes d'effacement adressées à l'exploitant n'étaient pas traitées. Outre la clarification de ce point, notre procédure vise également à vérifier si ce fournisseur respecte d'autres dispositions du droit de la protection des données, notamment en ce qui concerne les exigences de transparence et de sécurité du traitement et à l'éventuelle transmission de données personnelles à des tiers.

Le Préposé planifie de nouveaux portails de déclaration

Le Préposé prépare l'introduction de deux portails de déclaration en ligne pour l'annonce des pertes de données et la communication des coordonnées des conseillers à la protection des données prévues par la nouvelle LPD. La nouvelle LPD révisée fixe de nouvelles obligations de déclaration au Préposé, destinées aux responsables des traitements. Ces obligations portent sur l'enregistrement des activités de traitement par les organes fédéraux, la communication des coordonnées des conseillers à la protection des données et l'annonce des violations de la sécurité des données. Le Préposé souhaite simplifier au maximum les démarches en permettant des déclarations en ligne simples et sécurisées.

En premier lieu, le registre des fichiers déclarés au Préposé doit être adapté car dorénavant, seuls les organes fédéraux seront tenus de lui déclarer leurs registres des activités de traitement. Le portail de déclaration et de recherche www.datareg.admin.ch sera remanié en conséquence et conçu pour répondre aux nouvelles prescriptions.

De plus, deux nouveaux portails de déclaration seront créés. Le premier portail devra permettre une saisie structurée et efficace des conseillers à la protection des données nommés par les responsables des traitements. Ce portail est conçu sur le modèle d'une borne libre-service dans laquelle les responsables des traitements enregistrent, modifient et effacent eux-mêmes les coordonnées des conseillers à la protection des données. Le deuxième portail permettra de saisir les annonces des violations de la sécurité des données qui entraînent un risque élevé pour les personnes concernées, annonces dont le nombre devrait augmenter de l'avis du Préposé. Ce portail devrait également permettre une saisie simple et structurée, assurer une automatisation de l'évaluation des données rationnelle en termes de ressources et garantir une réaction en temps réel aux événements signalés.

La nouvelle loi sur la protection des données du point de vue du Préposé fédéral

Le secteur privé et les autorités fédérales ont jusqu'à l'entrée en vigueur de la nouvelle LPD (cf. encadré) pour adapter leur traitement de données personnelles aux nouvelles dispositions. Le 5 mars 2021, le Préposé a mis en évidence et publié les principales nouveautés dont ils devront tenir compte à cette fin (cf. notre communication «Nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT»). Il recommande de considérer en particulier les points suivants :

Uniquement les données des personnes physiques

Comme le RGPD, la LPD révisée vise exclusivement à protéger la personnalité des personnes physiques dont les données personnelles sont traitées – et non plus aussi les données des personnes morales, comme c'était le cas jusqu'ici.

Données personnelles sensibles

La définition actuelle des données personnelles sensibles est étendue aux données génétiques, ainsi qu'aux données biométriques si ces dernières identifient de manière univoque une personne physique.

Protection des données dès la conception et par défaut

Les principes de «protection des données dès la conception» et de «protection des données par défaut» sont désormais inscrits dans la LDP 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. Elles devront concevoir leurs applications de sorte que les données soient systématiquement anonymisées ou effacées. La protection des données par défaut protège les utilisateurs d'offres en ligne privées qui n'examinent ni 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.

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 désormais, le responsable du traitement privé devra 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. 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 Préposé fédéral préalablement au traitement (art. 23 LPD révisée). Au cas où le Préposé aurait des objections concernant l'analyse d'impact elle-même, il suggérera au responsable du traitement des précisions ou des ajouts.

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 Préposé 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 Préposé fondera par ailleurs 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.

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 adéquat de gestion de la protection des données.

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 énumère les indications que ce registre devra au moins contenir ; il devra par ailleurs être constamment tenu 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.

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


ABHOLEN / PICK UP

assurant un niveau de protection adéquat. Il publiera une liste à cette fin, liste déjà dressée par le Préposé 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.

Si une communication à l'étranger est prévue – ce qui inclut également le stockage sur des systèmes étrangers (cloud) –, les pays devront être indiqués, peu importe qu'ils offrent ou non un niveau de protection des données adéquat. Ici, la LPD va plus loin que le RGPD.

Devoir d'information consolidé

Afin d'atteindre l'objectif de transparence visé par la révision, l'art. 19 de la LPD révisée consolide le devoir d'informer pour les entreprises. Pour tout projet de collecte de données personnelles, le responsable du traitement privé devra informer au préalable et de manière adéquate la personne concernée, 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. Les entreprises devront donc vérifier et actualiser leur déclaration relative à la protection des données. Si le traitement entraîne une décision individuelle automatisée, le responsable du traitement devra, en vertu de l'art. 21 de la LPD révisée, informer la personne concernée et lui accorder le droit d'être entendu et le droit de vérification qui lui reviennent.

Droit d'accès de la personne concernée

La nouvelle LPD consolide le droit d'une personne de demander si des données personnelles la concernant sont traitées. L'art. 25 dresse une liste étendue des informations que le responsable du traitement devra au moins transmettre, par exemple la durée de conservation des données personnelles traitées.

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 dorénavant annoncer au Préposé les cas de violation de la sécurité des données entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'annonce au Préposé 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 si la personne concernée doit être informée de l'événement et de quelle manière.

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 qu'il les transmette à un tiers. La personne concernée pourra faire valoir ce droit gratuitement, sauf si la remise ou la transmission des données exige des efforts disproportionnés.

Renforcement des compétences de surveillance

Avec la révision de la LPD, le Préposé devra en principe enquêter sur toutes les infractions. Il pourra désormais rendre des décisions contre les traitements de données inadéquats et devra être consulté dans certains cas. À l'avenir, des amendes pouvant aller jusqu'à 250 000 francs seront possibles.

Enquête sur toutes les infractions aux prescriptions de protection des données

Le Préposé devra ouvrir d'office une enquête contre un organe fédéral ou une personne privée qui aura enfreint la nouvelle LPD (art. 49, al. 1, LPD révisée). L'actuelle LPD prévoit encore la restriction selon laquelle le Préposé ne peut mener une enquête d'office contre des personnes privées, établissement des faits compris, 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 Préposé pourra renoncer à ouvrir une enquête lorsque la violation est de peu d'importance (art. 49, al. 2, LPD révisée). Comme jusqu'ici, le Préposé pourra toujours renoncer à engager les 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. Il faut globalement partir du principe que même après l'entrée en vigueur de la nouvelle loi, le Préposé, du fait de ses ressources limitées, fixera des priorités dans le traitement des dénonciations suivant le principe d'opportunité.

Décisions

En vertu de l'art. 51, al. 1, de la LPD révisée, le Préposé pourra mener des procédures conformément à la loi fédérale sur la procédure administrative[1] 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.

Consultations

Le Préposé n'est ni une autorité d'approbation ni un organisme d'homologation des applications, produits, réglementations ou projets. La nouvelle loi prévoit cependant à plusieurs endroits que le responsable du traitement devra consulter le Préposé avant la clôture définitive de travaux en la matière et la réalisation de ses 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.

Prises de position spontanées et information du public

Excepté ses prises de position dans le cadre de consultations formelles, le Préposé restera libre de s'exprimer spontanément sur des technologies nouvelles, sur des phénomènes de numérisation ou sur les 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 (également dans le cadre d'enquêtes formelles).

Émoluments

L'art. 59 de la LPD révisée liste les prestations pour lesquelles le Préposé 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 types de protection des données et de celle des règles d'entreprise contraignantes. Les conseils généraux que le Préposé fournira à des personnes privées seront eux aussi soumis à des émoluments.

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, la violation des devoirs de diligence et la violation du devoir de discrétion seront punis sur plainte seulement. L'insoumission à une décision du Préposé sera en revanche poursuivie d'office. C'est en principe la personne physique responsable qui sera punie. L'entreprise elle-même pourra toutefois désormais 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.

Le nouveau droit n'accorde toujours pas de pouvoir de sanction au Préposé. Les contrevenants seront punis par les autorités cantonales de poursuite pénale. Le Préposé pourra dénoncer des infractions et faire valoir les droits d'une partie plaignante dans la procédure (art. 65, al. 2, LPD révisée), mais il n'aura pas le droit de porter plainte.

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

Le long chemin qui mène au but

Au cours de la session d'automne 2020, le Parlement fédéral a adopté la révision totale de loi fédérale sur la protection des données (LPD) et la modification d'autres actes législatifs connexes. Le Conseil fédéral devrait mettre en vigueur la nouvelle LPD et les ordonnances d'exécution y afférentes au second semestre 2022.

Historique

La première loi fédérale sur la protection des données du 19 juin 1992 est entrée en vigueur à l'été 1993. 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. 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 et les réseaux sociaux.
À l'automne 2017, le Conseil fédéral a adopté le projet de révision totale, qu'il a transmis à l'Assemblée fédérale.

Objectifs de la révision

Outre le renforcement des droits des personnes concernées, le Conseil fédéral met en avant dans son message une approche dite fondée sur le risque comme premier principe de la révision : 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 devrait également encourager l'autorégulation, dans la mesure où les membres des branches d'activité qui édictent un code de conduite contraignant sont dégagés de certaines obligations. Enfin, elle devrait renforcer les pouvoirs de surveillance du Préposé.

Consultation par étapes

Au début de l'année 2018, le Parlement a décidé de scinder la révision en deux étapes : dans un premier temps, les modifications ont touché les dispositions concernant les traitements de données applicables aux organes fédéraux tels que fedpol. Ces travaux ont abouti à la loi dite de protection des données Schengen entrée en vigueur le 1er mars 2019 (cf. 27e rapport, ch. .2).
Ce n'est que dans un second temps que la révision totale de la LPD dans son intégralité a eu lieu. Conseil prioritaire, le Conseil national s'est attelé à la révision totale de la loi au cours de la session d'automne 2019, révision que les Chambres fédérales ont adoptées 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'Europe[1], 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 un large pan 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.
Après le renouvellement de leur législation relative à la protection des données, la Suisse et l'UE devraient reconnaître réciproquement l'équivalence de leurs niveaux de protection des données, de sorte que l'échange informel de données personnelles restera possible par-delà les frontières. La décision européenne de reconnaissance à l'égard de la Suisse, la dernière datant de l'année 2000, était encore attendue au moment de l'achèvement de la rédaction.

[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 cette convention à l'été 2020. Le Conseil fédéral ne pourra le ratifier qu'après l'entrée en vigueur de la nouvelle LPD.

[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, RGPD).

1.2 Justice, Police, Sécurité

Demandes d'accès déposées auprès du Service de renseignement de la Confédération (SRC)

Après avoir été confronté à un nombre inhabituellement élevé de demandes d'accès en 2019, qu'il n'a d'abord pu traiter qu'avec un retard considérable, le SRC a pris des mesures particulières que le Préposé a accompagnées au titre de son activité de surveillance.

Fin 2019, divers médias ont rapporté que le SRC recevait un nombre beaucoup plus élevé que d'ordinaire de demandes concernant les inscriptions dans ses systèmes d'information. Cette hausse avait été provoquée, entre autres, par de précédents articles de presse titrant sur « l'espionnage » de personnalités politiques. Dans ce contexte, d'une part, la Délégation des Commissions de gestion (DélCdG) des Chambres fédérales a procédé à des investigations à ce sujet. Outre cela, l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) a examiné la tenue des dossiers concernant des personnalités politiques dans le système de gestion des affaires du SRC.

Après avoir été informé, par des plaintes émanant de citoyens, que le SRC accumulait de très importants retards dans le traitement des demandes d'accès, le Préposé est intervenu auprès du SRC qui lui a déclaré que depuis 2019, il avait reçu environ dix fois plus de demandes d'accès qu'à l'accoutumée : en un peu plus d'un an, il aurait reçu plus de 1000 demandes. Le SRC a alors assuré vouloir tout mettre en œuvre pour traiter les demandes en suspens en l'espace de quelques semaines. Il a également précisé qu'entretemps, il avait mis sur pied un groupe de travail chargé d'adapter les processus de travail de sorte que les nombreuses demandes en suspens soient traitées sans préjudice de la qualité.

En juin 2020, le SRC a informé le Préposé que grâce aux ressources supplémentaires allouées pour la réduction des demandes en suspens, les nouvelles demandes d'accès ont été traitées dans les délais depuis mai 2020. Le SRC précisait de plus que le nombre des demandes d'accès encore en attente (environ 50), car déposées à une date antérieure, diminuait régulièrement.

Le message sur la révision de la loi sur les profils d'ADN a été adopté

Par la révision de la loi sur les profils d'ADN, le Conseil fédéral entend permettre aux autorités d'extraire davantage d'informations d'une trace d'ADN au cours des enquêtes pénales. La revendication d'un cadre juridique strict formulée par le Préposé a été prise en compte.

Le Conseil fédéral a adopté le message concernant la modification de la loi sur les profils d'ADN le 4 décembre 2020. Il entend par là permettre aux autorités d'extraire davantage d'informations d'une trace d'ADN au cours des enquêtes pénales. Le 26 janvier 2021, à l'issue d'auditions détaillées, la Commission de la politique de sécurité du Conseil national (CPS-N) a décidé, sans opposition, d'entrer en matière sur le projet de loi. Elle estime que les autorités d'enquête disposeront ainsi de méthodes efficaces pour enquêter plus rapidement et de manière plus ciblée. La Commission souligne que le projet respecte le principe de la proportionnalité : il prévoit en effet que les résultats du phénotypage serviront exclusivement à élucider des infractions passibles d'une peine privative de liberté maximale de plus de trois ans. Dans la pratique actuelle, seul le sexe de l'auteur présumé peut-être déterminé à l'aide d'une trace d'ADN, et uniquement dans certains cas. Avec cette révision, il sera désormais possible d'autoriser la mise en évidence des probables couleurs des yeux, des cheveux et de la peau, origine bio-

géographique et âge des donneurs de trace. Comme l'a demandé le Préposé, les caractéristiques qui pourront être examinées seront fixées par la loi de manière exhaustive.

Le Préposé s'était déjà prononcé sur le projet de modification du Département fédéral de justice et police (DFJP) et avait demandé un cadre légal strict (à propos de la première consultation des offices, cf. 27e rapport d'activités, ch. 1.2). Au cours de la procédure de consultation, il avait précisé - comme il l'avait déjà fait dans le cadre de l'avant-projet - que le phénotypage et la recherche de parenté devaient être ordonnés par le tribunal des mesures de contrainte. Il s'agit en effet d'instruments qui ont une incidence considérable sur les droits fondamentaux et ne devraient être utilisés que pour enquêter sur des crimes graves contre l'intégrité physique, la liberté ou l'intégrité sexuelle. Le Préposé s'est félicité du fait que sa requête ait été prise en compte malgré le refus initial du DFJP.

Projet législatif concernant le contrôle des téléphones mobiles dans le cadre de la procédure d'asile

Le projet législatif lancé par l'initiative parlementaire 17.423 vise à élargir les compétences du Secrétariat d'État aux migrations (SEM) qui pourrait alors, dans le cadre des procédures d'asile et de renvoi, procéder au contrôle des supports de données mobiles afin d'établir l'identité des requérants. Le Préposé a exprimé très tôt des réserves fondamentales à ce sujet. Il approuve certes les améliorations apportées entre-temps, mais maintient son rejet de principe du projet législatif.

L'initiative parlementaire 17.423 déposée par le conseiller national Rutz le 17 mars 2017 demande une modification des bases légales permettant au SEM d'analyser les supports de données mobiles des requérants d'asile. Les commissions des institutions politiques des deux Chambres ont donné suite à cette initiative. C'est sur cette base qu'a été rédigée la modification de la loi sur l'asile et de la loi sur les étrangers et l'intégration, modification accordant au SEM des compétences étendues pour contrôler les supports de données mobiles en vue d'établir l'identité des requérants dans le cadre de la procédure d'asile et de renvoi.

Le Préposé s'est prononcé sur ce projet dans le cadre de la procédure de consultation et a exprimé des réserves fondamentales (cf. rapport du 04.06.2020 uniquement en allemand) . Il a ainsi souligné que constituant une ingérence massive dans la vie privée de nombreuses personnes, l'analyse des supports de données électroniques doit s'appuyer sur des bases légales formelles suffisantes. Le Préposé a également exprimé des doutes quant à la possibilité d'obtenir l'effet souhaité par les mesures proposées et, de surcroît, d'appliquer ces mesures dans le respect des droits fondamentaux relatifs aux principes constitutionnels d'égalité et de proportionnalité, cela d'autant plus que la procédure administrative d'asile et de renvoi, contrairement au droit pénal, ne connaît pas de garanties procédurales proprement dites en matière de saisie et d'analyse des supports électroniques de données. Ces mesures ne doivent pas non plus entraîner une contrainte indirecte à avoir sur soi un smartphone et à le rendre disponible à tout instant.

Les autorités concernées, dont le SEM en particulier, ont considéré ces critiques dans un esprit constructif et ont largement pris en compte les requêtes du Préposé. Par exemple, la confiscation des supports de données électroniques a été écartée et une base légale au sens formel a été créée. Comme l'a demandé le Préposé, il est désormais expressément précisé que l'analyse des supports de données mobiles en vue d'établir une identité est une mesure subsidiaire, qui doit toujours être proportionnée, et qu'il ne peut être tenu compte du refus du requérant de laisser inspecter son téléphone portable que dans le cadre de l'appréciation de la crédibilité. Les personnes concernées ont un

droit de présence et un droit d'information. La position des tiers dont les données personnelles sont également concernées par l'analyse a également été renforcée. Enfin, le Préposé se félicite du fait que ses préoccupations fondamentales quant à l'adéquation et à l'efficacité de la mesure envisagée soient prises en compte par le biais d'une obligation d'évaluation. Toutefois, le Préposé ne voit toujours pas comment les principes de subsidiarité et de proportionnalité seront appliqués dans la pratique. D'après le rapport explicatif sur la modification des bases légales, l'on cherchera toujours à établir l'identité par d'autres moyens dès lors qu'une autre mesure implique une charge de travail moindre qu'une analyse de données électroniques. L'appréciation de la proportionnalité d'une mesure devrait donc dépendre en définitive du choix de la procédure d'évaluation nécessitant la plus petite charge de travail. Il convient de rappeler à cet effet que, selon le projet de loi, l'analyse des données personnelles pourra être automatisée grâce à l'utilisation d'un logiciel adéquat. Par conséquent, l'évaluation des supports de données électroniques pourrait être effectuée de manière régulière, voire standard. Toutefois, l'efficacité ne doit pas être placée au-dessus du respect des libertés fondamentales. Le Préposé se doit donc de maintenir son rejet de principe du projet. Au-delà du contexte du droit d'asile, il souligne que les mesures de restriction de la liberté sont souvent d'abord introduites à l'encontre des minorités avant d'être progressivement étendues dans d'autres contextes à de larges pans de la population.

Intervention du Préposé auprès de l'Administration fédérale des douanes : insuffisance des dispositions sur le traitement des données dans la nouvelle loi sur la police douanière

L'Administration fédérale des douanes travaille à une révision de la loi dans le but d'établir le cadre légal nécessaire à l'utilisation des technologies numériques axées sur l'avenir et de créer en même temps la flexibilité organisationnelle permettant de réagir encore plus rapidement et efficacement aux changements de situation. Le Préposé se félicite de ces efforts, mais critique l'insuffisance des règles de traitement des données dans ce projet d'envergure.

Sous la désignation « loi fédérale sur les tâches d'exécution de l'OFDF », le Conseil fédéral a ouvert le 11 septembre 2020 la procédure de consultation sur un paquet législatif grâce auquel il entend créer la base légale du programme de numérisation et de transformation (programme DaziT) de l'Administration fédérale des douanes. Il s'agit d'un projet majeur, important financièrement et sensible quant à la protection des données. Il prévoit notamment le transfert de l'actuelle Administration douanière et du Corps des gardes-frontières, rattaché à cette dernière, vers un nouvel office de police douanière, l'Office fédéral de la douane et de la sécurité des frontières, l'OFDF. L'ensemble de son personnel sera doté de pouvoirs de police et donc de la compétence requise pour collecter des données de manière contraignante.

Lors de la seconde consultation des offices qui a eu lieu du 5 au 25 mars 2020 (à propos de la première, cf. 27e rapport, ch. 2.4), le Préposé a fait remarquer en vain à l'Administration fédérale des douanes que, selon lui, les dispositions prévues en matière de traitement des données personnelles présentent de graves lacunes. Il y manque en particulier la reconnaissabilité requise par la loi sur la protection des données, qui permettrait aux citoyens d'évaluer les traitements de données effectués par l'État empiétant sur leur vie privée et leur autodétermination informationnelle, ainsi que les droits de protection dont ils disposent à cet égard.

Le Préposé a recommandé à l'intention du Conseil fédéral que le Gouvernement et le Parlement, en tant qu'organes politiques de la Confédération, puissent se réserver le droit de régler les éléments essentiels des traitements de données, auxquels il faudrait procéder dans ce nouveau système d'information unique de police douanière, ainsi que ceux des interfaces avec ce système.

Sur la base de ces indications, le Conseil fédéral a chargé l'administration de réexaminer les dispositions relatives aux traitements de données, ainsi qu'il est mentionné dans le dossier relatif à la consultation. Le Préposé s'en félicite. Il est en contact étroit avec l'Administration fédérale des douanes et l'Office fédéral de la justice afin de remédier, sur la base de suggestions concrètes, aux manquements constatés.

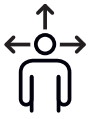
1.3 Fiscalité et finances

Le Préposé défend devant le Tribunal fédéral le droit à l'information dans l'assistance administrative internationale en matière fiscale

En 2019, le Tribunal administratif fédéral (TAF) avait admis le recours du Préposé concernant le droit à l'information dans le cadre de l'assistance administrative fiscale internationale. Dans la procédure de recours portée ensuite devant le Tribunal fédéral, le Préposé s'est de nouveau engagé en faveur du droit à l'information. La décision du Tribunal fédéral est encore attendue.

Dans l'assistance administrative fiscale internationale, le droit d'être informé d'une procédure d'assistance administrative en cours est lié au droit de recours d'une personne (cf. art. 14 de la loi sur l'assistance administrative fiscale). Fin décembre 2017, le Préposé a émis une recommandation formelle selon laquelle, dans le cadre de l'assistance administrative fiscale internationale, l'Administration fédérale des contributions (AFC) doit également informer les personnes non concernées par la demande d'assistance administrative (les tiers) dont les noms doivent être communiqués en clair à l'autorité étrangère requérante, donc sous une forme non caviardée (cf. 25e rapport d'activités, ch. 1.9.2), et cela avant la transmission des noms en question. Le Préposé estime en effet que les tiers ont le droit de se défendre au moyen d'un recours contre une communication illicite de leurs données. L'AFC a rejeté cette recommandation, à la suite de quoi le Préposé a d'abord soumis l'affaire au Département fédéral des finances (DFF), puis porté la décision négative du DFF devant le TAF (cf. 26e rapport d'activités, ch. 1.3).

Dans son arrêt du 3 septembre 2019, le TAF a conclu que, dans le cadre de l'assistance administrative internationale en matière fiscale, les personnes non concernées par la demande d'assistance administrative (les tiers), dont les données seront transmises non caviardées, doivent être en principe informées au préalable. Selon le TAF, il faut élaborer des dispositions dérogatoires pour les cas où les informations requises impliqueraient un effort disproportionné et rendraient impossible ou retarderaient de manière déraisonnable l'exécution de l'assistance administrative. Le Préposé s'est félicité de ce jugement car il protège les droits fondamentaux des employés de banque et autres tiers.



L'AFC a recouru devant le Tribunal fédéral. Celui-ci a levé la suspension de la procédure demandée par l'AFC après avoir rendu un arrêt de principe (ATF 146 I 172) le 13 juillet 2020 dans une autre affaire portant sur une question similaire. Dans cet arrêt, le Tribunal fédéral restreint fortement le droit à l'information : il précise que les tiers dont les données sont transmises par l'AFC à l'autorité étrangère requérante sans être caviardées n'ont qualité pour recourir qu'exceptionnellement, à savoir dans des situations très particulières. De plus, avant la transmission des données, l'AFC n'est pas tenue d'informer d'office tous les tiers habilités à recourir, mais seulement ceux dont la qualité pour recourir ressort de manière évidente du dossier.

Tenant compte de cette très récente jurisprudence, le Préposé a reconnu devant le Tribunal fédéral que les tiers ne sont pas habilités d'une manière générale à recourir dans le cadre de l'assistance administrative fiscale internationale, mais seulement dans des cas exceptionnels. Il a toutefois maintenu sa position, confirmée par le TAF, selon laquelle tous les tiers doivent être en principe informés d'office et préalablement à la transmission de leurs données. Ce n'est que de cette manière que tous les tiers habilités à recourir au sens de la jurisprudence du Tribunal fédéral peuvent effectivement exercer leur droit de recours et se défendre contre une transmission de données imminente. Le Préposé a ensuite développé une nouvelle fois, devant le Tribunal fédéral, comment une obligation fondamentale de renseigner de la part de l'AFC peut être mise en œuvre sans créer une charge disproportionnée pour celle-ci et sans retarder ou entraver excessivement l'assistance administrative internationale en matière fiscale. La décision dans cette affaire n'a pas encore été rendue.


Restaurants

1.4 Commerce et économie

Mise en œuvre de la 5G par Sunrise et Swisscom

Le PFPDT a mené à bien deux procédures distinctes d'établissement des faits auprès des sociétés Sunrise et Swisscom à propos du déploiement de la norme de technologie mobile de 5e génération (5G). Il en ressort que les deux fournisseurs accordent une grande importance à la protection des données et à la sécurité technique.

Selon les spécifications techniques, la 5G améliore à la fois la rapidité des données (débit) et la sécurité. Vu l'imminence et la portée de cette transformation, le Préposé a ouvert en 2019 deux procédures formelles d'établissement des faits auprès des sociétés Swisscom et Sunrise, qui prévoyaient alors toutes deux de lancer la 5G. Chacune a exposé au Préposé son plan de mise en œuvre et l'état d'avancement de celui-ci, documentation complète à l'appui. Outre de nombreuses questions techniques, le Préposé avait deux sujets de préoccupation majeurs : d'une part, la presse avait évoqué dès 2018 des faiblesses susceptibles d'apparaître lors de l'instauration de la 5G et l'existence de failles de sécurité connues; d'autre part, certains équipementiers, notamment Huawei, suscitaient des interrogations en matière de sécurité. Le Préposé a par conséquent demandé aux deux sociétés d'expliquer de quelle manière elles comptaient remédier aux faiblesses identifiées et de déclarer toute dépendance à l'égard de tel ou tel équipementier (en particulier Huawei) susceptible de nuire à la disponibilité des services (en raison de sanctions commerciales américaines, p. ex.), à la confidentialité ou à la sécurité des données.

Sunrise a démontré qu'elle pratiquait des échanges systématiques avec les organes internationaux et les groupes de travail du secteur des télécommunications et qu'elle soumettait en outre ses travaux de mise en œuvre au contrôle d'une société externe indépendante. Pour le Préposé, les mesures d'amélioration identifiées là sont particulièrement importantes pour l'obtention d'une sécurité suffisante et d'un niveau approprié de protection des données. Il a donc recommandé à Sunrise d'en mener à bien la réalisation. Sunrise a par ailleurs soumis son partenaire et équipementier en 5G Huawei à des analyses de risque, qui ont révélé des risques sur les plans de la disponibilité, de la coopération et de l'espionnage. Sunrise a défini et pris des mesures pour y remédier.

Chez Swisscom aussi, la mise en œuvre semble appropriée du point de vue de la sécurité et de la protection des données. La société a effectué des examens de sécurité internes pour s'en assurer. Comme Sunrise, Swisscom communique avec différents groupes de travail et organes internationaux et adopte les approches qui ont fait leurs preuves en matière de sécurité de l'exploitation. Swisscom a choisi son partenaire de longue date Ericsson comme équipementier principal pour la 5G et explique que les éléments fournis par Huawei pour la construction des antennes sont des composants passifs, non électroniques, servant uniquement à la réception et à l'envoi des signaux.

Le Préposé conclut de ses deux procédures que les deux sociétés respectent la sécurité des données et accordent une grande importance à leur protection. Le passage intégral à la 5G présente d'ailleurs en la matière des avantages certains par rapport à la 4G.

Saisies incorrectes dans la banque de données d'une société de recouvrement

Le Préposé a poursuivi la procédure d'établissement des faits concernant d'éventuelles écritures incorrectes dans les banques de données de l'une des principales sociétés de recouvrement de créances et a élargi le champ de l'enquête.

En février 2020, le Préposé avait engagé une procédure d'établissement des faits auprès de l'entreprise en question en raison d'écritures supposément incorrectes dans sa banque de données, de la confusion qui en était résultée entre des personnes ayant des noms et des adresses identiques ou similaires, ainsi qu'en raison des difficultés éventuelles à corriger ces entrées incorrectes (cf. 27e rapport, ch. 1.4). Au cours de l'année sous revue, il est apparu, à la suite de questions émanant de médias et de citoyens, que les cas de confusion de solvabilité négative dans un ménage (en allemand « negative Haushaltstreffer ») soulevaient également des questions relatives au droit de la protection des données. Le Préposé a donc décidé d'élargir à cet objet l'établissement des faits en cours. On parle de « confusion de solvabilité négative dans un ménage » lorsque des informations négatives sur la solvabilité d'autres personnes du même ménage sont communiquées dans le cadre d'un contrôle de la solvabilité. Ainsi, il se peut qu'un client potentiel ne puisse pas passer commande sur facture auprès de boutiques en ligne malgré une solvabilité irréprochable si une personne ayant une note de solvabilité négative vit dans son foyer. Ces clarifications juridiques étaient toujours en cours à la fin de l'année sous revue.

Vérification de la capacité à contracter un crédit pour un leasing automobile

Les clients désireux de conclure un contrat de leasing doivent donner leur consentement pour que le fournisseur de leasing vérifie leur solvabilité. Ce dernier peut aussi demander des renseignements à des tiers. Le Préposé procède aux premiers éclaircissements sur ces traitements de données.

Avant que les consommateurs puissent conclure un contrat de leasing pour une voiture, le fournisseur de leasing doit examiner leur solvabilité. À cette fin, il doit se procurer certaines informations sur les preneurs potentiels de leasing afin de disposer de renseignements sur leur situation économique. En cas d'évaluation négative, le contrat de leasing ne peut être conclu, conformément à la loi sur le crédit à la consommation, l'objectif étant d'empêcher le surendettement des consommateurs. Ces traitements de données sont soumis aux dispositions de la LPD et ne doivent pas porter une atteinte illicite à la personnalité du preneur de leasing ou d'éventuels tiers. En particulier, ils ne peuvent porter que sur les informations nécessaires à l'appréciation de la solvabilité.

Suite à des questions émanant de particuliers, le Préposé a appris que dans le but de vérifier la solvabilité de ses preneurs de leasing, un fournisseur de leasing leur réclamait un consentement lui permettant d'obtenir de nombreuses informations auprès de tiers. Ce consentement portait aussi sur l'obtention d'informations concernant des tiers tels que le conjoint ou des membres de la famille.

Pour le Préposé, la question se posait de savoir si ces traitements de données se limitaient à un niveau autorisé par la loi sur la protection des données et si la reconnaissabilité du traitement des données pour les personnes concernées était garantie. Le Préposé a donc demandé au fournisseur de leasing son avis sur différentes questions. En fonction de ses réponses, il examinera s'il doit procéder à une clarification et, le cas échéant, recommander des mesures.

Migros : procédure d'établissement des faits concernant la vidéosurveillance

Au cours de l'année sous revue, le Préposé a examiné le nouveau système de caméras de surveillance de Migros dans le cadre d'une procédure d'établissement des faits. L'entreprise a précisé que ce système n'impliquait ni reconnaissance faciale, ni évaluation automatisée des comportements ou autres analyses. Le Préposé n'a pas émis de recommandations, mais a requis que les clients soient mieux informés.

Pour les entreprises, les systèmes de vidéosurveillance peuvent être un moyen de sauvegarder leurs intérêts légitimes tels que la protection des biens. Mais de son côté, le public éprouve un malaise croissant à l'égard de ces projets, notamment en raison des nouvelles possibilités techniques d'identification et d'analyse.

Le nouveau système de Migros a également été critiqué dans les médias et a suscité un sentiment d'incertitude. Afin de clarifier les fonctions de la nouvelle vidéosurveillance de Migros, et dans le cadre de ses activités de surveillance, le Préposé a requis une description et une documentation concernant le système et les mesures de protection des droits de la personnalité.

Après avoir analysé le point de vue de Migros et les documents remis, le Préposé a constaté en premier lieu que le nouveau système de vidéosurveillance se limitait à des fonctions réactives : en cas de soupçon, le responsable de la sécurité d'une agence Migros peut enregistrer certains paramètres d'une personne suspecte (couleur des cheveux, sexe et taille) en sélectionnant manuellement une image fixe. Le système recherche la même combinaison de paramètres dans les séquences vidéo enregistrées et pour une période de temps définie. Les images sont montrées au personnel de sécurité du magasin Migros en question afin d'aider à identifier les agissements délictueux.

Migros a souligné qu'il n'y avait ni reconnaissance faciale, ni évaluation automatisée des comportements ou autres analyses. L'identification des personnes enregistrées par le système de vidéosurveillance n'est possible que dans des cas individuels justifiés en dehors du système et selon une procédure définie par l'entreprise.

Étant donné que le nouveau système de vidéosurveillance, du fait de ses fonctions limitées, ne présente pas de différence notable par rapport aux systèmes précédents, le Préposé peut s'abstenir de formuler des recommandations au regard de la loi sur la protection des données. En outre, les mesures et processus techniques et organisationnels décrits par Migros semblent à même d'assurer la sécurité des données personnelles traitées en rapport avec le système de vidéosurveillance.

Le Préposé a toutefois demandé à Migros d'améliorer, dans les dispositions relatives à la protection des données et sur son site Internet, les informations sur ce nouveau système car celles-ci sont formulées de manière trop générale et n'expliquent pas le nouveau système et ses fonctions. Il a en outre requis que Migros l'informe en temps voulu et au préalable de tout projet futur ou d'éventuelles extensions fonctionnelles dans le domaine de la vidéosurveillance. La réponse de Migros était encore attendue au moment de la mise sous presse du présent rapport.

Traitement de données de clients par les boutiques en ligne

Nous avons ouvert une procédure auprès d'une boutique en ligne afin de vérifier la conformité des traitements de ses données de clients avec la protection des données. La question se posait aussi de savoir si ces traitements peuvent avoir lieu contre la volonté expresse des utilisateurs.

Que ce soit en raison de la fermeture des commerces de détail pendant le confinement ou des risques liés aux achats en magasin, la pandémie de coronavirus a incité de nombreux clients à acheter en ligne. Pour certains, les magasins en ligne sont même devenus la seule possibilité de se procurer certains biens. Plusieurs demandes émanant de particuliers ont attiré notre attention sur le fait que pour passer une commande auprès de l'un des plus grands détaillants en ligne de Suisse, il fallait créer un compte client, donc accepter tous les traitements de données décrits dans la déclaration de protection des données du détaillant.

Cela signifiait notamment que les clients devaient consentir à l'enregistrement et à l'analyse de leur comportement d'achat sous une forme individualisée et personnalisée, à la mise en relation avec d'autres données personnelles (par ex. avec des données personnelles déjà collectées ou rendues publiques dans le passé par cette société, d'autres entreprises du groupe ou par des tiers) et à la transmission de données personnelles à d'autres sociétés du groupe. Les oppositions déposées ultérieurement au service clients n'ont pas permis d'empêcher ces traitements de données. L'exploitant de la boutique en ligne les a rejetées au motif que la déclaration de protection des données s'appliquait sans exception et de la même manière à tous ses clients et que les traitements de leurs données ne constituaient pas une option.

Dans l'optique d'une clarification préliminaire, nous avons écrit à l'exploitant de la boutique en ligne au printemps 2020, d'une part afin d'obtenir une vue d'ensemble de ses méthodes de traitement et, d'autre part, de clarifier les possibilités d'opposition des clients. Après examen de la réponse de l'exploitant, nous avons ouvert une procédure d'établissement des faits. Notre objectif est d'analyser les traitements de données effectués par l'exploitant de la boutique en ligne et par d'autres sociétés du groupe sous l'angle de leur conformité avec la protection des données. Nous nous concentrerons particulièrement sur la question de savoir si ces traitements de données peuvent avoir lieu contre la volonté expresse des utilisateurs.

Utilisation des données de Ricardo au sein du TX Group: notre appréciation juridique

Dans le cadre de la procédure en cours, le PFPDT a procédé à l'examen juridique de l'utilisation, au sein du TX Group, des données collectées sur la plateforme d'enchères en ligne ricardo.ch. Nous avons conclu que les traitements de données effectués aux fins de publicité ciblée du groupe devaient être justifiés par le consentement des utilisateurs. En outre, nous estimons que l'information transmise aux utilisateurs n'est actuellement pas suffisante et que la déclaration de protection des données doit être améliorée.

Dans le cadre de la procédure d'établissement des faits initiée à l'encontre de Ricardo et étendue à Tamedia/TX Group concernant l'utilisation des données collectées sur la plateforme d'enchères en ligne ricardo.ch au sein du TX Group, notre constatation des faits a pu être clôturée en mars 2020 (cf. nos précédents rapports d'activités). Celle-ci se base en particulier sur la nouvelle déclaration de protection des données de ricardo.ch – utilisée de manière standardisée par les sociétés du TX Group – ainsi que sur les réponses apportées par Ricardo et TX Group concernant les traitements des données effectués en leur sein. Dans le cadre d'un rapport final, nous avons procédé à l'appréciation juridique sous l'angle de la loi sur la protection des données (LPD).

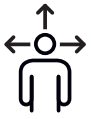
La déclaration de protection des données de Tamedia/TX Group, introduite en juillet 2017 pour ricardo.ch (actualisée plusieurs fois depuis), prévoit notamment que les données personnelles collectées sur la plate-

forme ricardo.ch peuvent être communiquées aux sociétés du TX Group ou à leurs partenaires et traitées « à des fins de personnalisation et de marketing ». Le comportement en ligne des utilisateurs peut notamment être suivi et évalué au travers d'outils d'analyse. Ce traitement de données reposerait « avant tout sur des données pseudonymisées ou anonymisées ». La finalité du traitement est d'adresser ou d'afficher sur les portails de TX Group de la « publicité anonyme » et d'améliorer la sécurité des portails.

Notre établissement des faits a permis d'établir que TX Group (anciennement Tamedia AG), traite et analyse certaines données des utilisateurs de la plateforme ricardo.ch à des fins de marketing. Les données collectées sur les différents portails de TX Group permettent d'enrichir, sous une forme agrégée, la base de données du groupe. La finalité de l'analyse et de la combinaison de ces données en provenance de sources diverses est d'adresser aux utilisateurs des services du TX Group ou à leurs partenaires de la publicité ciblée, selon une segmentation effectuée en fonction d'attributs socio-démographiques (selon les données fournies par l'utilisateur lors de l'enregistrement) et des centre d'intérêts présumés des utilisateurs (déduits de leur comportement en ligne sur les portails du TX Group ou d'autres sites partenaires). La combinaison des données au sein du TX Group est rendue possible au travers d'identifiants pseudonymes, créés notamment à partir de l'adresse e-mail.

Nous avons procédé à l'examen juridique de l'état de faits et sommes parvenus, entre autres, aux appréciations suivantes:

- Le traitement des données, en particulier la combinaison des données effectuée par le TX Group et l'attribution de segments aux utilisateurs, est bel et bien un traitement de données personnelles soumis à la loi fédérale sur la protection des données (LPD). En outre, l'ensemble des données résultant du profilage peut constituer en l'occurrence un profil de personnalité au sens de la LPD et les exigences accrues de protection de la loi s'appliquent ;



- Nous estimons qu'un tel profilage à des fins de publicité ciblée nécessite en l'occurrence le consentement des personnes concernées, qui doit être au surplus explicite. En effet, même si le TX Group peut se prévaloir d'intérêts légitimes, ceux-ci ne l'emportent pas dans le cas d'espèce sur le droit à l'autodétermination informationnelle des utilisateurs de la plateforme ricardo.ch ;
- La déclaration de protection des données de Ricardo/TX Group et la communication y relative doivent être améliorées, conformément au principe de transparence. En particulier, les utilisateurs doivent comprendre de manière non équivoque les traitements de données effectués par Ricardo d'une part, par TX Group d'autre part, quelles sont leurs finalités, s'il existe des moyens de s'y opposer ou non et, le cas échéant, les possibilités d'opposition doivent être réellement appliquées.

Nous sommes en train d'examiner les prochaines étapes.

Révision de l'ordonnance sur l'énergie

Dans le cadre de la révision de l'ordonnance sur l'approvisionnement en électricité (OApEl), le Préposé demande que la durée de conservation des données de mesure par les gestionnaires de réseau ne dépasse pas deux ans, ceci dans l'intérêt des personnes concernées. Le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) rejette cette demande en s'appuyant notamment sur la période de cinq ans figurant déjà dans l'ordonnance. Il y a divergence avérée entre ces deux positions.

Dans le cadre de la consultation des offices relative à la révision de l'ordonnance sur l'énergie, le Préposé a qualifié de disproportionner sur le plan temporel le délai de stockage de cinq ans des valeurs fournies par le dispositif de mesure de la courbe de charge prévu par cette révision. À ses yeux, il s'agit ici d'un cas de conservation de données touchant tous les consommateurs d'électricité en Suisse. Selon le projet, dans le dessein d'optimiser la consommation électrique, les profils de la courbe de charge seraient conservés durant cinq ans, bien qu'il soit fort probable que la majorité des personnes concernées ne les évaluent jamais.

Il existe d'autres moyens moins contraignants pour atteindre les buts poursuivis afin d'établir le bilan de la gestion du réseau et la facturation, par exemple une agrégation en fonction des positions tarifaires (par ex. tarif élevé/bas) pour la facturation, le profil de la courbe de charge en soi n'étant plus pertinent pour la facturation.

Selon l'OApEI, les données personnelles et les profils de personnalité sont détruits au terme de douze mois, à moins qu'ils ne soient pertinents pour la facturation ou anonymisés.

La longue période de conservation de cinq ans est particulièrement problématique car les profils de la courbe de charge sont des profils de personnalité ou, selon la nouvelle loi sur la protection des données, constituent du profilage, cas dans lequel des exigences accrues en matière de protection des données s'appliquent.

Le Préposé est donc d'avis que les données personnelles doivent être effacées au terme de douze mois ou, pour des raisons de praticabilité, au plus tard au terme de deux ans, à moins que les personnes concernées n'aient explicitement consenti à une durée de conservation plus longue qui permettrait, par exemple, de rassembler des informations sur les données des profils de la courbe de charge en vue d'améliorer l'efficacité énergétique. La disposition en question devrait être modifiée de manière à ce que la durée de conservation des profils de la courbe de charge soit de douze mois comme actuellement, et que les clients puissent demander une durée de conservation supérieure, jusqu'à cinq ans au maximum, sur la base d'un consentement explicite.

1.5 Santé

Exigences relatives aux solutions en nuage pour le traitement des données de patients

Dans le secteur des soins de santé, les solutions informatiques en nuage (cloud) sont de plus en plus utilisées pour le traitement des données de patients. Consulté à leur propos, le Préposé a mis en exergue les points dont les professionnels de santé doivent tenir compte au moment de choisir une solution informatique en nuage.

Au cours de l'année sous revue, le Préposé a été contacté à plusieurs reprises par des médecins, des psychologues et autres professionnels de santé à propos de l'utilisation de solutions informatiques en nuage pour le traitement des données de patients. Il s'agissait du traitement ou du stockage de données de santé dans un centre de données exploité par un fournisseur externe de services en nuage (cloud provider). Les questions portaient en particulier sur la conservation et la transmission, ou l'effacement, des données de patients (par ex. après le décès d'un patient ou la fermeture d'un cabinet médical).

Dans le cadre de ses activités de conseil, le Préposé rappelle en premier lieu que le médecin demeure responsable de la sécurité des données lorsqu'il opte pour une solution informatique en nuage bien que, dans ce cas, il n'ait plus qu'un contrôle limité sur la sécurité des données. Il doit donc choisir avec soin son fournisseur de services en nuage et prêter attention aux points suivants :

- les données doivent rester en Suisse ;
- le contrat avec le fournisseur de services en nuage doit répondre aux exigences posées par le secret médical ;
- toutes les personnes ayant accès aux données du patient doivent être soumises au secret médical ;
- il doit être possible à tout moment d'effacer les données de patients ;
- il doit être possible à tout moment de fournir la liste de toutes les personnes qui ont accès aux données ;
- la sécurité des données doit être régulièrement vérifiée et les audits s'y rapportant doivent être disponibles ;
- l'interlocuteur pour la protection des données doit être connu du médecin ;
- une sauvegarde quotidienne doit être possible ;
- toutes les connexions doivent être cryptées et une double authentification doit restreindre l'accès aux données aux seules personnes autorisées.

En conclusion, pour l'échange ou le stockage de données de patients, le Préposé déconseille donc d'utiliser les systèmes gratuits et courants d'informatique en nuage, car ils ne remplissent généralement pas les conditions précitées.

CORONA

mesvaccins.ch : procédure d'établissement des faits

La plateforme électronique mesvaccins.ch, créée plusieurs années avant la pandémie de COVID-19, était exploitée par une fondation avec le soutien financier de l'OFSP notamment. Elle était pressentie pour devenir le pendant électronique du carnet de vaccination.

Pendant la crise, la plateforme a vu le nombre de ses utilisateurs croître fortement grâce, entre autres, aux interfaces avec l'application d'inscription à la vaccination diffusée par l'OFSP. La fondation exploitait en outre un module spécifique de documentation des vaccinations contre le COVID-19 (myCOVIDvac), qu'elle avait développé sur mandat de l'OFSP.

Fin mars 2021, le préposé a pris connaissance des résultats d'une enquête journalistique selon lesquels mesvaccins.ch présenterait des failles de sécurité et des atteintes graves à la protection des données. Après avoir consulté le Centre national pour la cybersécurité (CNCS), il a ouvert le jour même une procédure formelle d'établissement des faits en recommandant à la fondation de suspendre immédiatement l'exploitation du site. À la fin de l'exercice, la procédure était toujours en cours et la date de reprise de l'exploitation impossible à prévoir.

Par ailleurs, le préposé a fait en sorte, en concertation avec les autorités cantonales de protection des données, que les plateformes exploitées par des entreprises privées dans le cadre de la lutte contre la pandémie, sur mandat ou sur la recommandation des autorités sanitaires de la Confédération ou des cantons, soient soumises à un contrôle plus strict.

CORONA

Allégement des mesures pour les personnes vaccinées : enjeux du point de vue du droit de la protection des données

Le lancement de la vaccination contre le coronavirus a fait naître un débat public sur la levée des interdictions et des mesures de restriction des libertés pour les personnes vaccinées. Le PFPDT a déclaré publiquement dès décembre 2020 que le traitement des données de santé par l'État et par l'économie dans le cadre de l'allégement des mesures pour les vaccinés devait se faire selon des dispositions claires de droit public, sans entraîner aucune obligation de porter un smartphone sur soi.

Le lancement de la vaccination contre le coronavirus a fait naître, au cours de la deuxième vague de la pandémie, un débat public sur la levée des interdictions et des mesures de restriction des libertés pour les personnes vaccinées. Les Commissions des institutions politiques (CIP) des deux chambres ont réfléchi aux modalités juridiques de cet allégement en auditionnant différents acteurs, dont le préposé (cf. communiqué de presse de la CIP-E du 23.02.2021).

L'État et les acteurs privés qui effectuent des tâches étatiques ne peuvent différencier les personnes selon qu'elles sont ou non vaccinées qu'en se fondant sur une base légale appropriée. Entre particuliers, ce type de différenciation est licite de toute façon en vertu de la liberté du contrat.

Lorsqu'un acteur privé fait dépendre l'accès à des biens ou des services du statut vaccinal de ses clients, il est amené à traiter régulièrement des données relatives à la santé de ses concitoyens, ce qui implique, selon les circonstances, un risque d'atteinte à la personnalité. C'est la raison pour laquelle le préposé a appelé, dès le commencement du débat public et lors des auditions évoquées, à la création de bases légales dans ce domaine.

Il a en outre rappelé les dispositions du droit de la protection des données que les acteurs privés doivent respecter s'ils veulent subordonner l'accès à des biens ou à des services à la présentation d'un test négatif ou d'une attestation de vaccination (cf. communiqué du 22.01.2021).

Le principe de la proportionnalité veut que l'acquisition et le traitement des données personnelles soient en adéquation avec la finalité poursuivie, c'est-à-dire la protection contre la transmission et la maladie. Il ne faut contraindre personne à fournir des données sur sa santé pour obtenir des biens ou des services dont il ne peut pas se passer. S'agissant des modalités du traitement, le préposé estime qu'il faut proposer aux personnes qui ne peuvent ou ne veulent pas présenter leur certificat de vaccination sur un smartphone des solutions de remplacement raisonnables qui permettent de traiter leurs données personnelles dans des conditions comparables.

Ce dernier aspect est d'autant plus important à ses yeux que selon toute vraisemblance, le traitement systématique de données personnelles par des acteurs privés qui s'est généralisé dans le contexte de la pandémie aura des répercussions sur l'autodétermination de la population en matière d'information bien au-delà de la crise actuelle.

CORONA

Certificat COVID : mise en œuvre conforme à la protection des données

Compte tenu de la nécessité, pour pouvoir se rendre à l'étranger, de prouver que l'on a été vacciné contre le COVID-19 ou qu'on en est guéri, ou de présenter un résultat de test négatif, le Parlement fédéral a créé en mars 2021 une disposition légale prévoyant un certificat sanitaire uniforme, infalsifiable et reconnu sur le plan international. Le préposé participe aux travaux de mise en œuvre de l'Office fédéral de la santé publique (OFSP) dans le cadre de son devoir de consultation.

Au cours de la seconde vague de la pandémie est apparue la nécessité, principalement pour les personnes souhaitant se rendre à l'étranger, mais pas uniquement, de disposer d'un document fiable attestant qu'on a été vacciné contre le COVID-19, qu'on est guéri de la maladie, ou que l'on a été testé négatif au coronavirus. Il n'existait pas alors en Suisse de dispositions légales spécifiques sur la forme et le contenu d'un carnet de vaccination. L'attestation en question était proposée sous différentes formes (document papier, SMS, courriel ou inscription [vérifiable] sur une plateforme dédiée), or toutes n'étaient pas conformes au droit de la protection des données, ce qui a amené le PFPDT à intervenir en vertu du droit de la surveillance (cf. encadré).

En mars 2021, le législateur fédéral a prévu, dans le nouvel art. 6a de la loi COVID-19, la création d'un certificat sanitaire uniforme et reconnu sur le plan international prouvant que son titulaire a été vacciné contre le COVID-19, qu'il en est guéri ou qu'il dispose d'un résultat de test de dépistage. Ce document doit être personnel, infalsifiable et, dans le respect de la protection des données, vérifiable ; il doit être conçu de manière que seule une vérification décentralisée ou locale de son authenticité et de sa validité soit possible et qu'il puisse, dans la mesure du possible, être utilisé par son détenteur pour entrer dans d'autres pays et en sortir. Il sera disponible sous forme électronique et sur papier, ce qui satisfait le préposé, qui craignait que l'instauration d'un certificat exclusivement numérique ne conduise à une obligation générale de porter un smartphone sur soi.

La disposition prévoit en outre que la Confédération pourra mettre à la disposition des cantons et de tiers un système pour la délivrance du document. Chargé de développer un tel système, l'OFSP a créé à cette fin, le 29 mars 2021, un groupe de projet que le préposé accompagne en vertu de son devoir légal de consultation. Les exigences du préposé quant au respect du droit de la protection des données recoupent l'avis conjoint du Comité européen de la protection des données (EDPB) et du Contrôleur européen de la protection des données (CEPD) concernant le «certificat vert numérique» qui doit être mis en place dans l'UE pour la circulation transfrontalière. Le préposé a par ailleurs formulé à l'intention du groupe de projet des prescriptions relevant du droit de la protection des données afin que les certificats comportent un minimum de données en vue d'autres usages éventuels en Suisse. Il estime que pour ces usages, il faut créer des bases de droit public ciblant non seulement les autorités mais aussi les acteurs privés (cf. texte ci-dessus).

Dossier électronique du patient: les premières communautés de référence ont été certifiées

Toutes les régions de Suisse s'apprêtent à lancer le dossier électronique du patient (DEP). Le PFPDT a suivi le développement des procédures de certification. Pour ce faire, il a intensifié ses échanges avec les communautés de référence. Certaines ont déjà franchi le cap de la certification.

Le DEP est un recueil virtuel de liens permettant aux particuliers d'accéder à la version numérique de leurs données de santé telles que les rapports médicaux ou les ordonnances. Il s'agit de données personnelles sensibles dont le traitement nécessite le consentement exprès de l'intéressé, ce qui suppose qu'il ait reçu à ce sujet des informations claires et complètes. Le Préposé accorde à ce dernier aspect une importance capitale. Au cours de l'année sous revue, il a eu l'occasion de consulter les documents émis à ce sujet par des communautés de référence.

La loi fédérale sur le dossier électronique du patient (LDEP) entrée en vigueur le 15 avril 2017 laisse le patient maître des droits d'accès aux éléments de son dossier. Il faut donc que soient correctement définis les niveaux de confidentialité de chaque document, l'attribution d'un rôle d'utilisateur à certains professionnels de la santé, les suppléances et le paramétrage selon lequel en cas d'urgence, l'accès des professionnels de la santé traitants est subordonné à leur habilitation préalable. Le Préposé est particulièrement attentif à cet aspect des choses et continuera d'observer la gestion des autorisations, notamment à l'issue de la procédure de certification des communautés de référence, afin que les patients gardent le contrôle de leurs données même après avoir donné leur consentement. Il reste en contact à ce sujet avec l'Office fédéral de la santé publique, les fournisseurs de l'infrastructure technique et les autorités cantonales de protection des données. Ces échanges permettent notamment de régler certaines questions de compétence qui découlent du fait que certains prestataires médicaux tels que les hôpitaux relèvent des autorités cantonales de protection des données, tandis que les médecins et les communautés de référence sont soumis à la surveillance du PFPDT.

Il était prévu que les communautés de référence soient mises en service en avril 2020, mais la procédure de certification a pris du retard. « eHealth Aargau (SteHAG) » fut la première communauté de référence à obtenir, à la mi-novembre 2020, la certification prévue par la LDEP. La communauté de référence sud-est de l'association « eSANITA » fut la seconde, fin décembre 2020. Le Préposé les a invitées toutes deux à exposer les principaux risques pour la protection des données qu'elles ont identifiés en rapport avec le DEP, les mesures qu'elles envisagent pour y remédier et les moyens par lesquels elles assument leurs responsabilités quant au droit de la protection des données.

Les principaux interlocuteurs du Préposé à cet égard seront les responsables de la protection et de la sécurité des données nommés par les communautés de référence en vertu de la LDEP.

CORONA

Application de traçage de proximité de la Confédération (application SwissCovid)

Dès le début de la pandémie de coronavirus, le Préposé a été contacté à titre consultatif par les développeurs du système de traçage de proximité à l'origine de l'application SwissCovid de la Confédération. Ce système utilise la technologie Bluetooth pour déterminer les rapprochements pertinents du point de vue épidémiologique entre téléphones portables et les enregistre localement. Le Préposé a suivi de près le développement de l'application SwissCovid, d'abord du point de vue technique, puis du point de vue législatif aussi.

Le 21 mars 2020, quelques jours après la déclaration de situation extraordinaire en Suisse au sens de la loi sur les épidémies (LEp), les développeurs d'une application de traçage de proximité Covid ont contacté le Préposé et l'ont prié d'évaluer cette application sous l'angle de la protection des données. Issus de l'École polytechnique fédérale de Lausanne (EPFL) et du secteur privé, ils visaient une application permettant d'avertir les personnes ayant activé l'application Covid sur leur smartphone qu'elles s'étaient trouvées à proximité d'une autre personne possédant un appareil similaire doté de cette application et dont le test de dépistage du coronavirus s'était ultérieurement révélé positif. Dans sa première évaluation, le Préposé a constaté que le projet tenait compte d'importantes préoccupations en matière de protection de la vie privée et d'autodétermination informationnelle de par les choix de ne pas collecter les données de localisation (à l'origine prévu), de recourir à des identificateurs temporaires et de garantir le caractère volontaire de la participation.

Par la suite, l'EPFL et ses partenaires ont développé leur application sous le nom de Decentralized Privacy Preserving Proximity Tracing (DP-3T). Ces travaux ont été réalisés indépendamment du projet européen Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) et ont apporté des améliorations en matière de protection des données, notamment par l'introduction d'une approche décentralisée du traitement des données. En particulier, nous avons jugé positif que le serveur central, également indispensable dans l'approche décentralisée, reçoive uniquement des clés anonymes et que les approches épidémiologiquement pertinentes ne soient enregistrées sur les smartphones que localement.

Au fil de l'avancement du projet, la Confédération a décidé d'introduire un système de traçage officiel basé sur le modèle DP-3T. Dès lors, l'Office fédéral de la santé publique (OFSP), responsable du projet, nous a associés aux travaux de mise en œuvre de la future application SwissCovid de la Confédération et les a très largement documentés. Cela a permis à nos spécialistes de vérifier du point de vue technique l'application et l'architecture de son système, y compris la mise en œuvre dans le back-end. En mai, le Préposé a estimé, sur la base notamment d'une analyse d'impact sur la protection des données, que les conditions préalables prévues par la loi sur la protection des données pour la réalisation d'un essai pilote étaient remplies (cf. prise de position du Préposé du 13 mai 2020).

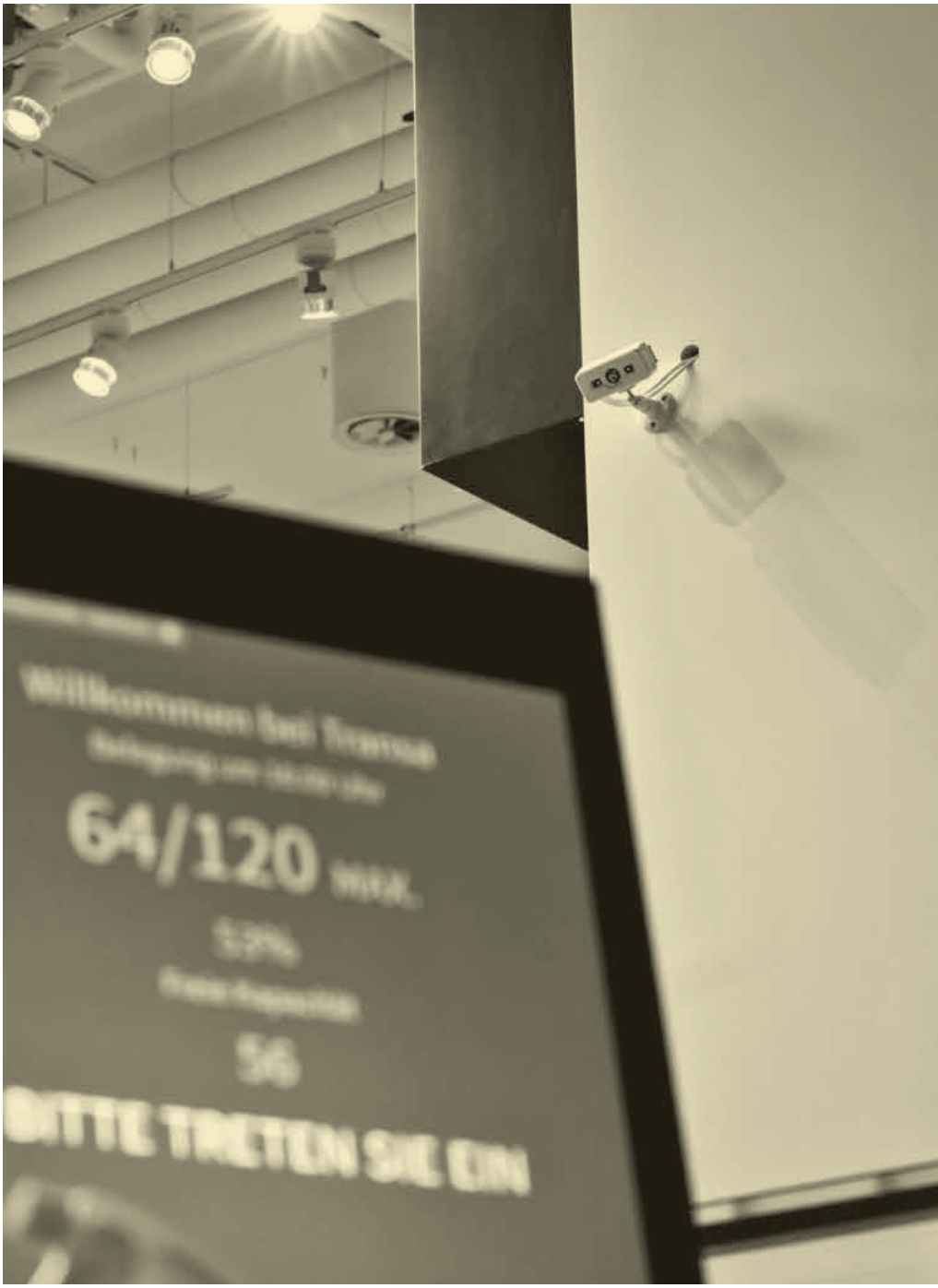
Après examen d'un rapport publié en juin par le Centre national pour la cybersécurité (NCSC), le Préposé a confirmé cette appréciation. Il a souligné que l'utilisation des interfaces de programmation d'applications (API) de Google et d'Apple pour l'application SwissCovid, utilisation critiquée par les médias et les milieux proches de la protection des données, ne constituait pas un risque significativement supérieur par rapport à l'utilisation quotidienne de ces interfaces par la population.

Après avoir demandé sans succès à l'administration d'introduire pour cette application une base légale suffisamment concrète dans la LEp conformément à l'art. 17 LPD, le Préposé a pu conseiller les commissions parlementaires compétentes dans le sens de la création d'une base légale, laquelle a été concrétisée par l'introduction urgente d'un nouvel article 60a dans la loi sur les épidémies le 25 juin 2020 (cf. art. 60a LEp).

Selon cette disposition, la participation à l'application SwissCovid est volontaire. D'une part, le législateur était conscient qu'une obligation

aurait été difficilement acceptée du point de vue politique et qu'en outre, elle n'aurait guère été applicable car la fonction Bluetooth peut être désactivée à tout moment. D'autre part, en interdisant aux autorités, aux entreprises et aux particuliers d'avantager ou de désavantager quiconque en fonction de l'utilisation ou de la non-utilisation de l'application, le Parlement a clairement signalé qu'il rejetait l'obligation de facto d'avoir sur soi un smartphone.

Le 25 juin 2020, l'application SwissCovid a été lancée dans les boutiques d'applications mobiles d'Apple et de Google. Si, des mois plus tard, une partie de la population est encore très méfiante à l'égard de cette application quant à son respect de la protection des données, d'autres voix s'élèvent pour accuser le législateur d'avoir trop limité son efficacité par la prise en compte de la protection des données. Pris entre ces deux positions contradictoires, l'OFSP n'a pas été en mesure d'accroître la diffusion de l'application au-delà du volume certes considérable - mais en-deçà des attentes optimistes - de quelque 3 millions de téléchargements et 1,7 million d'utilisateurs actifs.



CORONA

Le cadre légal de la collecte des coordonnées

Par ses interventions, le Préposé a contribué à ce que la collecte des coordonnées pour le traçage des infections au COVID-19, le « traçage des contacts », repose sur des bases légales suffisamment précises et respecte ainsi les principes de la loi sur la protection des données.

Lors de la réouverture le 11 mai 2020 des restaurants, bars, discothèques, centres de fitness et autres installations accessibles au public,

de nombreux établissements avaient prévu la collecte de coordonnées pour le traçage des infections dans le cadre des plans de protection ordonnés par le Conseil fédéral. Comme il n'existait à l'origine aucune base légale pour la collecte et la transmission de ces données, le Préposé a pris position publiquement afin que, momentanément, elles aient lieu uniquement sur une base volontaire (cf. notre communication du 19.05.2020 « Coronavirus : plans de protection »).

Par son intervention, le Préposé a pu contribuer à ce que le Conseil fédéral établisse une base légale suffisamment précise régissant l'obligation de relever les coordonnées des clients. Celle-ci a été introduite le 22 juin 2020. Dans l'« ordonnance COVID-19 situation particulière », le Conseil fédéral a délimité la finalité de l'utilisation des données collectées (transmission à l'autorité cantonale compétente à des fins de recherche des contacts en cas d'infection), réglé les exigences attachées à leur conservation (garantie de la confidentialité) et à l'effacement automatique après 14 jours, et défini les catégories de données à collecter au niveau fédéral (nom, prénom, domicile et numéro de téléphone).

Afin d'améliorer l'efficacité du traçage des contacts, certains cantons ont obligé les exploitants de restaurants à utiliser une application spécifique pour collecter les coordonnées de leurs clients. Outre la nécessité de disposer d'une base légale (cantonale) claire, le Préposé a souligné que les applications en question doivent garantir que le traitement des données est identifiable, sûr et en adéquation avec la finalité poursuivie. Il a également rappelé à plusieurs reprises que les acteurs privés ne doivent pas imposer à leurs clients une obligation factuelle de

détenir un smartphone. Tout d'abord, certaines personnes ne veulent pas d'un smartphone équipé d'un programme précis parce qu'elles craignent que l'on accède à des informations concernant leur vie numérique. Par ailleurs, d'autres ne sont pas du tout en mesure d'utiliser ce genre d'appareil en raison de leur âge, de leur santé ou d'un handicap. En parallèle à ces méthodes numériques d'obtention des données, les entreprises privées doivent donc aussi mettre à la disposition de ces personnes, à des conditions acceptables, d'autres moyens de collecter les coordonnées tels que les listes papier.

Enfin, depuis l'été 2020, les problèmes d'ordre juridique et technique liés à l'utilisation de certaines applications pour la collecte des coordonnées se sont accumulés. Le Préposé a donc décidé d'ouvrir une procédure d'établissement des faits à propos d'une application largement utilisée dans plusieurs régions de Suisse. Il souhaite terminer cette enquête avant la réouverture du secteur de la restauration, ce qui constitue un défi de taille compte tenu des formalités de la procédure.

1.6 Secteur du travail

Admissibilité des vérifications d'antécédents dans les processus de recrutement

De plus en plus d'entreprises, essentiellement étrangères, offrent aux employeurs suisses la possibilité de passer au crible des bases de données pour y trouver des informations sur les candidats à un poste et formuler ensuite une recommandation d'embauche. Le Préposé a été consulté à plusieurs reprises à propos de l'admissibilité de ces vérifications d'antécédents.

Conformément à l'art. 328b CO, l'employeur ne peut traiter que les données nécessaires au processus de recrutement en question. Ce faisant, l'employeur doit toujours respecter les principes de traitement des données de la LPD, en particulier le principe de proportionnalité et le principe de transparence.

Le principe de proportionnalité exige que l'exploration de bases de données et l'évaluation ultérieure des données consultées soient appropriées, nécessaires et raisonnables afin de vérifier les qualifications des candidats. Un contrôle de sécurité plus ou moins étendu relatif aux personnes peut être approprié, nécessaire et raisonnable dans les domaines où les employés ont accès à des informations sensibles, ceci afin de limiter certains risques, comme dans les secteurs bancaire ou sécuritaire. En revanche, en l'absence de risques particuliers, comme c'est vraisemblablement le cas à propos des enseignants par exemple, sous réserve de circonstances particulières, un contrôle de sécurité complet paraît disproportionné.

Indépendamment de la question de la proportionnalité, l'employeur est tenu, en vertu de l'obligation de transparence, d'informer la personne concernée de la vérification de ses antécédents ainsi que du traitement des données et des évaluations la concernant. C'est seulement ainsi que cette personne peut vérifier la licéité du traitement des données et l'exactitude des données, ou faire valoir ses droits. Compte tenu du devoir de transparence, les vérifications d'antécédents secrètes et donc non communiquées aux personnes concernées sont illicites.

CORONA

Télétravail et protection des données

Au cours de l'année sous revue, de nombreux employés ont été obligés de travailler à domicile. Le Préposé s'est donc penché avec une plus grande attention sur les questions concernant l'utilisation de divers systèmes de visioconférence, la surveillance des collaborateurs et l'accès aux serveurs des entreprises suisses à partir de l'étranger.

Les conditions permettant d'introduire le télétravail à domicile pour les salariés sont définies par le droit du travail. Du point de vue de la protection des données, cette possibilité soulève toutefois un certain nombre de questions non négligeables, par exemple touchant à l'utilisation de moyens de communication numériques pour les conférences téléphoniques et les visioconférences (voir à ce sujet l'encadré au ch. 1.1 du présent rapport), ou l'utilisation de plateformes d'échange de données. Même si les obligations des salariés peuvent changer de manière ponctuelle, en temps de crise aussi l'employeur demeure responsable de la sécurité de l'information et de la protection des données ; il est donc lié par les principes de traitement des données de la LPD. Dans cette perspective, il lui incombe de choisir un logiciel garantissant de manière adéquate la sécurité des données personnelles traitées. Sous le titre « Mesures de sécurité pour les conférences audio et vidéo », le Préposé a publié sur son site Internet un feuillet thématique énumérant les principales règles en matière de protection des données à appliquer au moment du choix des plateformes requises.

Plusieurs demandes émanant de particuliers portaient sur la crainte d'être exposé, durant le télétravail, à la surveillance permanente de l'employeur. Le Préposé est conscient que, selon la solution informatique utilisée, le comportement des employés en télétravail pourrait être aisément surveillé en permanence - ce qui est toutefois inadmissible au regard de la LPD et de plus, expressément interdit en vertu des normes du code du travail.

Enfin, le Préposé a été confronté à plusieurs reprises à la question de savoir s'il y a divulgation de données vers l'étranger lorsque l'employé est en télétravail à l'étranger - que ce soit dans une résidence de vacances ou, dans le cas des frontaliers, à leur domicile - et accède de cet endroit au serveur de l'entreprise en Suisse. Toutefois, tant que l'employé accède au serveur de l'entreprise depuis son lieu de séjour à l'étranger via un réseau privé virtuel (VPN), qu'il traite les données personnelles uniquement dans la mesure où il le ferait en temps normal dans les bureaux de l'entreprise et surtout qu'il ne rend ces données accessibles à personne à l'étranger, cela ne constitue pas une communication transfrontière de données au sens de la LPD. Que les employés soient en télétravail à l'étranger ou en Suisse, la confidentialité des données personnelles doit toujours être garantie.

CORONA

Exigences en matière de protection des données concernant la détection précoce du coronavirus sur le lieu de travail

La pandémie de COVID-19 a soulevé diverses questions touchant les conditions de travail, par exemple à propos de la conformité avec la protection des données de diverses mesures telles que l'admissibilité des contrôles de température sur le lieu de travail, ou de la communication interne sur les infections détectées. La question s'est posée à plusieurs reprises de savoir si les mesures en question étaient proportionnées.

Dans le cadre d'un rapport de travail, l'employeur ne peut traiter que les données concernant l'employé et nécessaires à l'exécution du contrat de travail. Le principe de proportionnalité conformément à la LPD doit toujours être pris en considération. Ainsi, tout traitement de données doit être approprié, nécessaire et acceptable afin d'atteindre le but recherché - en l'occurrence, prévenir les infections sur le lieu de travail.

À propos des mesures de température sur le lieu de travail, la question s'est posée de savoir si cette vérification est réellement appropriée pour limiter les contagions. D'une part, une forte température peut être le symptôme d'une autre maladie ; d'autre part, la température corporelle peut être aisément abaissée de manière artificielle par la prise de médicaments. En outre, tous les porteurs du virus ne présentent pas de symptôme de fièvre. Ainsi, un contrôle général de la température semble n'être qu'en partie approprié à la prévention des infections sur le lieu de travail. L'employeur devait se demander s'il n'existait pas d'autres mesures moins radicales pouvant mener au même but. Dans chacun de ces cas, le Préposé a conseillé que les employés soient tenus de prévenir immédiatement une personne de confiance de l'entreprise en cas d'apparition des symptômes typiques d'une infection au coronavirus. Dans son appréciation du problème, le Préposé s'est aussi appuyé sur les recommandations de la task-force scientifique suisse COVID-19 qui déconseille expressément le contrôle de la température en tant que mesure isolée et préventive.

L'autre question régulièrement soulevée a été celle de savoir comment un employeur doit ou peut communiquer un cas d'infection au reste du personnel, cela afin de permettre aux employés qui ont été en contact avec la personne infectée de se mettre en quarantaine. L'employeur a un devoir de diligence envers ses salariés exigeant que ces informations soient traitées, même si la recherche des contacts est en principe du ressort des autorités cantonales compétentes (médecin cantonal) et non de l'employeur.

1.7 Assurances

Instauration du système d'informations et de renseignements HIS contre la fraude à l'assurance

L'Association Suisse d'Assurances (ASA) a consulté le PFPDT à propos de l'instauration du système d'informations et de renseignements HIS, une base de données contre la fraude à l'assurance. Le Préposé a insisté sur le fait que tout traitement de données réalisé dans le cadre de l'exploitation du HIS devait respecter le principe de la proportionnalité inscrit dans le droit de la protection des données.

La consultation du Préposé au sujet du HIS a commencé dès la période 2017/2018 (cf. 25e rapport d'activités, ch. 1.6.2).

Les compagnies d'assurance affiliées inscrivent dans cette base de données les personnes pour lesquelles des irrégularités ont été constatées lors du règlement d'un sinistre (réticence au sens de l'art. 6 de la loi fédérale sur le contrat d'assurance, p. ex.). Si une personne est impliquée dans un nouveau sinistre, l'assureur voit apparaître dans le système la mention des irrégularités antérieures, ce qui lui fournit un élément important pour apprécier son devoir de prestation. Les motifs d'inscription dans le HIS peuvent relever du droit des contrats d'assurance ou de celui de la responsabilité civile, mais non du droit pénal. Une compagnie d'assurance ne peut savoir si une personne y figure que si celle-ci est impliquée dans un nouveau sinistre ; elle ne peut en aucun cas le vérifier en dehors du processus de règlement des sinistres (avant la conclusion d'un contrat, p. ex.). L'inscription concerne non seulement l'assuré mais aussi d'autres personnes impliquées le cas échéant (« complices » ou « instigateurs », p. ex.).

Lors de sa consultation, le Préposé a insisté sur le fait que tout traitement de données réalisé en rapport avec le HIS devait respecter le principe de la proportionnalité inscrit dans le droit de la protection des données. L'inscription dans le HIS doit être appropriée et nécessaire pour empêcher et pour révéler les fraudes à l'assurance, et l'atteinte à la sphère privée qu'elle implique doit rester acceptable pour l'intéressé. Il faut restreindre les motifs d'inscription et en donner une définition claire, qui assure leur transparence. L'inscription doit permettre à l'assureur de procéder à l'examen approfondi des prétentions de l'assuré en cas de nouveau sinistre, mais elle ne doit en aucun cas conduire à une condamnation anticipée. Des précautions s'imposent, par conséquent, pour garantir l'exactitude des données personnelles. Si des compagnies d'assurance multiplient les inscriptions injustifiées au mépris du règlement, il faut pouvoir les identifier et les sanctionner.

L'ASA a mis en œuvre la plupart des suggestions du Préposé. Elle a notamment précisé les motifs d'inscription. En fin de compte, c'est la pratique qui révélera si le HIS contribue à prévenir la fraude à l'assurance, dans quelle mesure les assureurs respectent la réglementation et si le droit de la protection des données exige des modifications.

Communication de données de membres à des sponsors

Pour le Préposé, la communication de données à des sponsors n'est licite qu'en présence d'un consentement valable. Les membres d'associations doivent donc pouvoir s'opposer à la communication de leurs données sans subir de préjudice disproportionné.

Au cours de l'année sous revue, le Préposé a reçu diverses demandes concernant la communication, à des sponsors, de données concernant les membres d'associations (en l'occurrence des adresses), ceci à des fins publicitaires. La question était de savoir s'il est permis de facturer une cotisation plus élevée aux membres qui s'opposent à la transmission de données. Nous avons indiqué aux personnes et aux associations concernées qu'il y a préjudice disproportionné si l'augmentation de la cotisation est si élevée que les personnes concernées se sentent pratiquement obligées d'accepter la communication de leurs données.

Le Préposé a déjà attiré l'attention des associations sportives et des sponsors sur leur responsabilité quant à la licéité des traitements de données qu'ils effectuent (cf. 22e rapport d'activités, ch. 1.8.5). Les associations ne sont pas autorisées à transmettre à des sponsors des données concernant leurs membres sans le consentement valable des personnes concernées. Pour qu'une communication de données soit licite, toutes les personnes concernées doivent avoir été informées au préalable, et de manière adéquate, du transfert considéré (c'est-à-dire quelles données seront transférées à quels destinataires et à quelles fins) et doivent pouvoir l'approuver. Si le consentement prend la forme d'une option de retrait (opt-out), il est essentiel que les membres puissent facilement s'opposer au partage de leurs données sans subir de préjudice disproportionné. Les sponsors, quant à eux, doivent garantir sur le plan contractuel qu'ils ne traitent que les données d'adresses des membres de l'association qui leur ont été transmises sur la base d'un consentement effectif.

Utilisation systématique du numéro AVS par les autorités: modification de la loi approuvée par le Parlement

Le 18 décembre 2020, le Parlement a approuvé la modification de la loi fédérale sur l'assurance-vieillesse et survivants. Celle-ci définit un large cercle d'autorités, organisations et personnes habilitées à utiliser systématiquement le numéro AVS à 13 chiffres (NAVS13) comme identifiant unique en dehors du domaine des assurances sociales. Des garanties importantes en matière de protection des données ont été obtenues par le Préposé.

Le 1er février 2017, le Conseil fédéral a chargé le Département fédéral de l'intérieur (DFI) de procéder à une consultation sur l'utilisation du NAVS13 de manière systématique par les autorités fédérales, cantonales et communales. Un groupe de travail interne à l'administration, auquel nous n'avions pas été convié, considérait alors qu'il n'y avait pas de risque particulier en matière de protection des données. Or, tant le PFPDT que les préposés cantonaux s'opposaient déjà au principe de l'utilisation systématique du NAVS13 en raison des risques en matière de protection des données.

Nous avons donc requis, conjointement à l'Office fédéral de la justice (OFJ), une évaluation sur les risques d'une utilisation systématique du numéro AVS, laquelle a été confiée au Prof. David Basin, professeur ordinaire à l'EPF de Zurich. Les conclusions de cette évaluation du 27 septembre 2017 soulignaient que l'utilisation systématique du NAVS13 présentait des risques non négligeables en matière de protection des données (cf. 25e rapport d'activités, ch. 1.1.2). L'expert recommandait l'utilisation de numéros sectoriels. Toutefois, il soulignait également qu'une telle mesure n'aurait pas les effets escomptés en matière de protection des données, sans que d'autres mesures importantes, comme le renouvèlement de l'architecture des bases de données, ne soient adoptées.

Suite à cette expertise, la Commission des affaires juridiques du Conseil national a déposé un postulat (17.3968) le 20 octobre 2017 invitant le Conseil fédéral à montrer dans un concept de quelle manière il était possible de faire face aux risques liés à l'utilisation du NAVS13 en tant qu'identifiant unique des personnes. Le concept devait en outre montrer de quelle manière la protection des données pouvait être améliorée dans le cadre de l'utilisation de numéros d'identification de personnes par les cantons, les communes et des tiers et prendra pour cela en considération l'avis du PFPDT. Dans sa réponse du 20 décembre 2017, le Conseil fédéral s'est dit conscient des risques potentiels liés à l'usage du NAVS13 et a déclaré prendre en compte l'étude Basin et les remarques du Préposé dans son projet de loi.
Lors de la pré-consultation des offices, nous avons demandé avec succès plusieurs modifications du projet, notamment celle de soumettre toutes les entités légitimées à utiliser systématiquement le NAVS13 à l'obligation de procéder à des analyses des risques et à l'obligation de tenir une liste des bases de données dans lesquelles le NAVS13 est enregistré. De même, la nécessité de renforcer les mesures techniques et organisationnelles visant à limiter les risques d'atteinte à la protection des données a été reconnue et intégrée au projet de loi (cf. 27e rapport d'activités, ch. 1.7).

Le 7 novembre 2018, le Conseil fédéral a ouvert la consultation sur la modification de la loi sur l'AVS, laquelle prévoit l'utilisation systématique du NAVS13. Toutefois, le projet a pris en considération les exigences du Préposé relatives à la protection des données. Une autorité peut lier des données factuelles (nom, prénom, date de naissance, etc.) au NAVS13 et vérifier leur exactitude auprès de la base de données Unique Person Identification (UPI) gérée par la Centrale de compensation (CdC). Cependant, elle ne peut pas accéder aux autres registres, à savoir le registre central des assurés et le registre des prestations de la CdC, ni aux registres contenant des données factuelles tenus par d'autres

autorités. Ceci permet d'éviter qu'une autorité soit en mesure de faire des liens entre différentes bases de données et d'établir des profils, par nature très précis, de la personnalité sur la base du NAVS13. Ainsi, il est à saluer que toutes les entités fédérales et cantonales, mais aussi les unités décentralisées de l'administration fédérale et les organisations et les personnes de droit public ou de droit privé qui sont extérieures aux administrations disposant de telles bases de données, doivent procéder périodiquement à des analyses de risques, en tenant compte notamment, du danger d'appariements non autorisés de données. Sur la base de cette analyse des risques, des mesures de sécurité et de protection des données adaptées à la situation de risque et correspondant à l'état de la technique doivent être définies et mises en œuvre. Les entités désignées par le projet de loi utilisant systématiquement le NAVS13 ont l'obligation de tenir un registre des banques de données pertinentes servant en particulier de base aux analyses de risques. Outre les administrations fédérales, cantonales et communales, les entités autorisées par la loi à utiliser le NAVS13 de manière systématique sont les établissements de formation, les entreprises d'assurances privées (aussi dans la cadre de l'assurance complémentaire) et les organisations et les personnes de droit public ou de droit privé extérieures aux administrations précitées et qui sont chargées de tâches administratives par le droit fédéral, cantonal ou communal ou par contrat, si le droit applicable prévoit l'utilisation systématique du numéro AVS. En outre, le NAVS13 ne doit pas être utilisé à des fins purement privées. Cela s'applique également dans le cas où les personnes concernées consentent à l'utilisation systématique de leur NAVS13 par des privés.

En plus des mesures précitées, nous saluons que la loi prévoit également des mesures techniques et organisationnelles contraignantes visant à se prémunir contre d'éventuelles utilisations abusives du numéro AVS. Ainsi le principe de l'accès aux banques de données contenant le NAVS13 inscrit dans la loi doit être limité aux personnes qui ont besoin de ce numéro pour accomplir leurs tâches. De même, les transmissions de fichiers comprenant le NAVS13 doivent se faire sous forme cryptée via le réseau public des fichiers de données. Enfin, une manière de procéder en cas d'accès non autorisé aux banques de données ou d'utilisation abusive de celles-ci devra être établie par les autorités, organisations et personnes habilitées à utiliser le numéro AVS et leur personnel devra être formé à utiliser le numéro AVS conformément à la loi. Des manquements à ces devoirs pourront être sanctionnés pénalement.

Suite à la procédure de consultation, le projet n'a par la suite plus été modifié de manière notable. En décembre 2020, peu avant le vote final de l'Assemblée fédérale, le parlement a élargi la liste des entités autorisées à utiliser systématiquement le NAVS13 en y intégrant les organes chargés de l'exécution des contrôles prévus par une convention collective de travail déclarée de force obligatoire.

Les multiples auditions du Préposé par les commissions parlementaires au cours du processus législatif ont permis de mettre le thème de la protection des données au cœur des dispositions légales. L'entrée en vigueur de ces nouvelles normes n'est pas attendue avant la fin de l'année 2021.

1.8 Transports

Forte augmentation des questions de la population concernant les drones

Au cours de la période sous revue, les demandes de renseignements de particuliers à propos des drones ont fortement augmenté. Ces demandes émanent tout autant de propriétaires de drones que de personnes s'estimant incommodées par les prises de vue effectuées par drones.

Les drones rencontrent apparemment un succès grandissant dans l'espace privé. Tout au moins, le Préposé a enregistré durant l'année sous revue une forte augmentation des demandes de particuliers à ce sujet. D'une part, il s'agit de personnes qui désirent faire des photos ou des enregistrements vidéo à l'aide d'un drone et souhaitent clarifier les exigences légales (en matière de protection des données) avec le Préposé et avec d'autres autorités (notamment l'Office fédéral de l'aviation civile OFAC). D'autre part, certains particuliers se sentent aussi dérangés par les drones qui tournent autour de leur domicile ou de leur lieu de travail, réalisant éventuellement des enregistrements sonores et visuels.

Ces citoyennes et citoyens sont nombreux à souhaiter que le Préposé leur communique sa position dans l'affaire les concernant, outre ses conseils juridiques. Dans ces cas, le Préposé rappelle que les principes généraux de la protection des données doivent être respectés et que pour traiter des données, les particuliers doivent avoir un motif justificatif. Pour les autorisations ou les interdictions, il renvoie aux autorités compétentes, en particulier l'OFAC, et aux tribunaux civils et pénaux cantonaux.

Nous avons publié sur notre site Internet, sous forme de feuillet thématique, de plus amples informations concernant la vidéosurveillance effectuée par des particuliers à l'aide de drones.

Révision de la loi sur le transport de voyageurs : il faut éviter les sources de discrimination pour les personnes empruntant les transports publics de manière anonyme

Le Préposé s'est exprimé dans le cadre de la « Consultation des offices concernant le message relatif à la modification de la loi sur le transport de voyageurs - une base moderne pour les transports publics ». Depuis cette consultation, plusieurs réunions ont eu lieu avec des représentants de l'Office fédéral des transports et de l'Office fédéral de la justice, au cours desquelles a notamment été discutée la question de savoir dans quelle mesure les entreprises de transport devaient être soumises aux dispositions de protection des données applicables aux particuliers ou aux autorités publiques.

Le Préposé a relevé en particulier que, dans le cas où les responsables de traitement privés sont soumis aux dispositions en vigueur, outre le consentement, les autres motifs justificatifs prévus par la LPD, tels que la base légale ou un intérêt prépondérant, sont disponibles. Par exemple, les entreprises de transports peuvent invoquer un intérêt prépondérant si elles traitent des données en relation directe avec la conclusion ou l'exécution d'un contrat.

Si le traitement des données est basé sur un consentement, il convient de respecter les conditions de la validité juridique de ce consentement : celui-ci doit être volontaire et précédé d'une information adéquate et transparente. Lorsqu'il s'agit de données personnelles sensibles et de profils de la personnalité, le consentement doit être explicite. En outre, le transport de personnes ne peut être subordonné au consentement à ce traitement des données en vue d'autres fins. Pour le traitement des données à des fins supplémentaires, des consentements distincts doivent être donnés par les personnes concernées.

Même lorsque le consentement implicite est suffisant, des informations complètes doivent être fournies afin que les clients puissent identifier les atteintes à la personnalité et qu'ils aient véritablement le choix d'opter soit pour l'offre accumulatrice de données, soit pour une autre offre anonyme à des conditions comparables. S'ils choisissent la solution accumulatrice de données, il y a alors consentement implicite. Le Préposé a également précisé que les offres alternatives anonymes ne doivent pas être liées à des obstacles financiers ou administratifs dissuasifs ou discriminatoires. Étant donné qu'un report intégral des

surcoûts des offres alternatives peut, le cas échant, conduire à l'exclusion de fait d'une partie de la population, le Préposé a demandé que la disposition en question de la loi sur le transport de voyageurs soit complétée en conséquence et que les motifs en soient précisés dans le message.

En ce qui concerne l'infrastructure de distribution, c'est-à-dire la plateforme centrale de commande, qui n'est pas encore mise en œuvre, le Préposé a attiré l'attention sur les principes généraux applicables dès maintenant, ainsi que sur les nouvelles exigences à respecter en vertu de la LPD entièrement révisée, exigences qui doivent être prises en compte lors du déploiement de la plateforme numérique, par exemple les nouvelles technologies et préréglages permettant de protéger les données (protection des données dès la conception et protection des données par défaut), et la protection des données persistantes.

Le Préposé continuera à accompagner le processus législatif et à œuvrer pour que les exigences en matière de protection des données soient prises en considération.

Utilisation des données des passagers des compagnies aériennes dans la lutte contre le terrorisme

Le Département fédéral de justice et police (DFJP) travaille actuellement à l'élaboration d'un projet législatif permettant à la Suisse d'utiliser les données des passagers des compagnies aériennes afin de lutter contre le terrorisme et la criminalité. Le Préposé est membre du comité d'experts externes de ce projet.

Le 12 février 2020, le Conseil fédéral a pris une décision de principe relative à l'utilisation en Suisse des données des passagers des compagnies aériennes (données PNR, pour Passenger Name Record) afin de lutter contre le terrorisme et la criminalité. À cette fin, le DFJP a été chargé de prendre les premières mesures nécessaires à la mise en place d'un système PNR national (cf. 27e rapport, ch. 1.2, p. 27). Le DFJP a maintenant pour mandat de préparer d'ici la mi-2021, en collaboration avec le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), un projet de consultation sur une loi fédérale relative à la collecte et à l'utilisation des données PNR par la Suisse et à leur transfert aux États dont la protection et le traitement des données répondent aux normes de la directive PNR de l'UE (directive (UE) 2016/681 du 27 avril 2016 relative à l'utilisation de données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière). De plus, également d'ici la mi-2021, le DFJP et le Département fédéral des affaires étrangères (DFAE) doivent préparer un mandat de négociation avec l'UE en vue d'un accord sur l'échange d'informations relatives aux données PNR entre les unités de coordination compétentes (Unités d'Informations Passagers/UIP) en Suisse et dans les États membres de l'UE.

Le Préposé siège au sein du comité d'experts externes du projet PNR et suit l'évolution de celui-ci sous l'angle du droit de la protection des données. La mise en place d'un système PNR ne doit permettre une limitation des droits fondamentaux que dans la mesure nécessaire aux fins envisagées. L'équilibre entre la garantie des droits fondamentaux et les restrictions indispensables pour assurer la sécurité publique doit être préservé. Cela implique notamment que la transmission de données soit effectuée selon la méthode dite « push » qui bloque l'accès direct à ces données pour les autorités étrangères. Conformément à sa pratique établie de longue date, le Préposé préconise également l'élaboration d'une liste d'infractions. Cette mesure répond au principe de proportionnalité et garantit la transparence.

En cas de communication de données vers les États-Unis, le bouclier de protection ne garantit pas aux personnes concernées en Suisse un niveau de protection adéquat.

Lors de son examen annuel, le Préposé a réévalué la conformité du bouclier Suisse-États-Unis (Swiss-US Privacy Shield) aux prescriptions légales en matière de protection des données, à la lumière de la très récente jurisprudence de la Cour de justice de l'Union européennes (CJUE) sur la question. Sa conclusion : le bouclier Suisse-États-Unis n'offre pas un niveau de protection suffisant aux personnes concernées en Suisse ; il invite donc les entreprises suisses à procéder au cas par cas à une estimation des risques lorsque la communication des données vers les États-Unis s'appuie sur des garanties contractuelles.

Dans ses rapports d'évaluation suivant les examens 2018 et 2019 du bouclier Suisse-États-Unis, le Préposé avait déjà souligné que, malgré les améliorations apportées depuis son entrée en vigueur, ce bouclier ne fournissait pas aux personnes concernées en Suisse des droits justiciables suffisants en cas d'accès aux données par les autorités américaines (cf. 27e rapport, p. 34 et 26e rapport, ch. 1.2). Il avait notamment critiqué le fait que l'efficacité du mécanisme dit du Médiateur, censé garantir une voie de recours indirecte, ne pouvait pas être évaluée en raison du manque de transparence. D'autre part, pour le Préposé, il n'était pas prouvé que les prérogatives décisionnelles du Médiateur à l'égard des Services de renseignement américains ainsi que son indépendance effective étaient suffisantes. Le Préposé avait jugé problématique ce manque de transparence et l'absence de garanties en cas d'ingérence des autorités américaines dans la vie privée des personnes en Suisse.

Le 16 juillet 2020, dans son arrêt en l'affaire C311/18 Data Protection Commissionner contre Facebook Ireland Ltd et Maximilian Schrems (arrêt dit Schrems II), la CJUE a invalidé la décision d'adéquation (UE) 2016/1250 concernant les entreprises américaines certifiées au titre du bouclier de protection. En outre, la CJUE a précisé que l'utilisation de clauses contractuelles types (CCT) pour les États-Unis et les autres pays tiers ne disposant pas d'une protection adéquate des données nécessitait une évaluation au cas par cas de leur adéquation et, si nécessaire, un complément.

Cet arrêt n'a pas d'effet contraignant pour la Suisse. Toutefois, selon le RGPD, le droit européen de la protection des données et la jurisprudence de la CJUE fondée sur ce droit peuvent aussi être appliqués par les autorités et les tribunaux de l'Union européenne, ou de l'EEE, aux établissements suisses lorsqu'ils traitent des données de sorte que celles-ci entrent dans le champ d'application du RGPD. Après une analyse approfondie de l'arrêt de la CJUE et de la situation juridique suisse, le Préposé a conclu dans sa prise de position du 8 septembre 2020 (cf. notre communiqué de presse) que le bouclier de protection Suisse-États-Unis n'offrait pas un niveau de protection adéquat au sens de la LPD pour la communication de données de la Suisse vers les États-Unis, bien qu'il garantisse aussi certains droits de protection particuliers aux personnes concernées en Suisse. Sur la base de cette évaluation, fondée sur le droit suisse, le Préposé a supprimé pour les États-Unis la mention « Niveau adéquat sous certaines conditions » dans sa liste des États. Cette liste est indicative. À l'heure actuelle, il n'existe pas en Suisse de jurisprudence comparable à l'arrêt de la CJUE précité. Une appréciation différente par les tribunaux suisses est réservée.

Les garanties contractuelles utilisées en plus du bouclier de protection pour les communications de données vers les États-Unis et d'autres pays tiers sans décision d'adéquation, telles que les CCT de l'UE également souvent utilisées en Suisse ou encore les « Binding Corporate Rules », n'empêchent pas les autorités étrangères d'accéder aux données personnelles dès lors que le droit public de l'État importateur prévaut et permet aux autorités d'accéder aux données personnelles transférées

sans garantie suffisante en matière de transparence et de protection juridique indépendante pour les personnes concernées.

Dans sa prise de position précitée du 8 septembre 2020, le Préposé a voulu sensibiliser les milieux économiques à ce problème. Il a indiqué quelques premières solutions possibles telles que le cryptage ou l'anonymisation totale.

Le Préposé invite les entreprises suisses à procéder à un examen des risques au cas par cas pour les transmissions de données vers les États-Unis qui s'appuient sur des garanties contractuelles. Ce n'est que sur la base de cet examen des risques qu'une entreprise peut juger si un transfert de données vers les États-Unis est conforme aux exigences de la protection des données et, le cas échéant, le documenter de manière pertinente pour le Préposé. L'UE élabore actuellement de nouvelles CCT. Le Préposé suit ces travaux et s'exprimera à leur sujet en temps voulu.

1.9 International

Introduction

Au cours de l'année écoulée, la coopération internationale a été marquée par la crise du COVID-19 et il a été pratiquement impossible d'organiser des rencontres in situ. Les conférences ont été soit annulées, soit tenues par liaison vidéo, ce qui n'a pas été sans poser des difficultés techniques, surtout au début. Grâce aux économies de coûts et de temps réalisées, certaines de ces visioconférences ont été suivies par un bien plus grand nombre d'autorités de protection des données, et de personnes par autorité, que d'ordinaire. En revanche, les discussions et les contacts informels essentiels à la coopération ont été quasiment inexistants. La crise a fait ressortir l'importance des échanges entre les autorités de protection des données au niveau international.

Le flux transfrontière de données n'a cessé d'augmenter - notamment en raison de la pandémie - soit par la communication directe de données personnelles à l'étranger, soit par le stockage de données dans des nuages et sur des serveurs à l'étranger. Pour les personnes concernées, il est souvent difficile d'évaluer quelles entreprises et autorités traitent leurs données à l'étranger. Il est dès lors d'autant plus important d'agir pour une meilleure mise en œuvre de la protection des données au niveau international, de promouvoir la coopération internationale entre les autorités de protection des données et de veiller à une compréhension commune et à une interprétation uniforme des normes et directives internationales.

L'harmonisation des directives au niveau international permet de garantir les mêmes droits aux personnes concernées, quel que soit leur lieu de résidence. Les autorités de protection des données doivent également se consulter au niveau international quant à la manière de répondre, sur le plan technique et dans la conception pratique de leurs activités de conseil et de contrôle, aux défis mondiaux en matière de protection des données tels que le Big Data, l'Internet des objets et l'intelligence artificielle.

Le Préposé continue d'être présent au niveau international et joue un rôle actif dans diverses instances internationales, dont le Conseil de l'Europe, les Conférences européenne et internationale des commissaires à la protection des données et de la vie privée, l'Association francophone des autorités de protection des données, l'OCDE, sans oublier la coopération et la coordination entre les autorités de protection des données des États membres de l'espace Schengen et les contacts avec le Comité européen de la protection des données (CEPD).

Conseil de l'Europe

Le Comité consultatif de la Convention 108 a tenu six sessions à distances sur différents thèmes. Il a adopté des lignes directrices sur la protection des données personnelles des enfants dans un cadre éducatif ainsi que des lignes directrices sur la reconnaissance faciale. La réunion plénière à également procédé à l'élection du Bureau.

Lors des dates initialement prévues pour la 40e réunion plénière du Comité qui a dû être reportée du fait de la crise sanitaire, le Bureau du Comité de la Convention 108 et l'Unité protection des données ont organisé des sessions à distance ouvertes à tous pour présenter les travaux du Comité à un public plus large que celui des délégations qui participent habituellement aux réunions à Strasbourg. Six sessions thématiques précises et éclairantes ont eu lieu les 1, 2 et 3 juillet :

- Session 1 : comment s'assurer que les pays engagés par la Convention 108+ respectent ses exigences ? Pourquoi un mécanisme de suivi et d'évaluation est-il nécessaire et lequel ?
- Session 2 : comment aborder les derniers défis posés par le profilage à l'ère de l'intelligence artificielle ?
- Session 3 : qu'implique le droit à la protection des données personnelles dans le contexte éducatif ? Que doivent faire les écoles et qu'est-ce qu'elles ne doivent plus faire ?
- Session 4 : les programmes d'identité numérique sont-ils développés selon le principe de la protection des données dès la conception (« privacy by design ») ?
- Session 5 : les miroirs de nos âmes : retenir les leçons de Ciceron et aborder les risques de la reconnaissance faciale.
- Session 6 : campagnes politiques et élections : pourquoi la protection des données est cruciale.

Le Comité consultatif a pu tenir sa 40e réunion plénière initialement prévue du 1er au 3 juillet par visioconférence du 18 au 20 novembre 2020. Lors de sa réunion, il a adopté le texte révisé des lignes directrices sur la protection des données personnelles des enfants dans un cadre éducatif. Ces dernières énoncent les principes fondamentaux des droits de l'enfant dans le cadre éducatif et ont pour but d'aider les législateurs et décideurs politiques, mais aussi les responsables de traitement des données et l'industrie à respecter ces droits. Il a également procédé à l'élection de son Bureau et a entre autres élu une représentante du PFPDT en la personne de Caroline Gloor Scheidegger, cheffe du domaine de direction relations internationales.

Suivant une procédure écrite, le Comité de la Convention 108 a également adopté les lignes directrices sur la reconnaissance faciale. Celles-ci contiennent des orientations pour les législateurs et décideurs en mentionnant entre autres l'implication nécessaire des autorités de contrôle. D'autre part, elles servent également à orienter les développeurs, fabricants et fournisseurs de services en précisant entre autres que la fiabilité des outils utilisés dépend de l'efficacité de l'algorithme. La troisième orientation s'adresse aux entités utilisatrices de technologies de reconnaissance faciale en mentionnant également leur responsabilité en procédant à une analyse d'impact sur la protection des données et en garantissant la protection des données dès la conception (« privacy by design »). Finalement, les lignes directrices précisent que tous les droits, tels que le droit à l'information, le droit d'accès, le droit à l'information en cas de décision individuelle automatisée, le droit d'opposition et le droit de rectification sont garantis aux personnes concernées.

Assemblée mondiale pour la protection de la vie privée

La 42e Assemblée mondiale pour la protection de la vie privée (AMVP), anciennement nommée Conférence internationale des commissaires à la protection des données et de la vie privée, s'est tenue du 13 au 15 octobre 2020, pour la toute première fois en ligne.

La 42e session à huis clos de l'Assemblée mondiale pour la protection de la vie privée (AMVP) a été ouverte par Elizabeth Denham, commissaire à l'information du Royaume-Uni, qui a souligné le travail effectué ces dernières années par l'AMVP pour moderniser son assemblée, définir son orientation stratégique et renforcer ses capacités afin de relever les défis liés au COVID-19 en 2020.

Cette année, l'événement était divisé en trois sessions en ligne, chacune d'entre elles étant suivie d'une discussion. Plus de 100 membres ont participé à cette importante réunion annuelle.

Le premier jour de la conférence a été consacré en particulier à l'examen des progrès réalisés dans le cadre du plan stratégique de l'AMVP convenu lors de la 41e conférence internationale de l'année dernière à Tirana, et notamment à l'examen des principales réalisations quant aux trois priorités stratégiques qui y avaient été définies, à savoir: faire progresser le respect de la vie privée à l'échelle mondiale à l'ère numérique, maximiser la voix et l'influence de l'AMVP sur la scène internationale et renforcer ses capacités.

Le deuxième jour de l'événement a été dédié aux défis liés à la pandémie de COVID-19. A ce titre, le rôle et la contribution essentiels du groupe de travail COVID-19 de l'AMVP y ont été soulignés. Les activités de celui-ci ont été discutées et les résultats spécifiques de ses travaux ont été présentés, notamment le compendium des meilleures pratiques en réponse au COVID-19 qui aborde, par exemple, le thème du traçage des contacts.

Le premier sujet abordé lors de la troisième journée a été l'avenir de la conférence. Ensuite, les résultats du vote des membres sur les rapports des groupes de travail, le rapport du Comité exécutif 2020 et le rapport de la 41e Conférence internationale 2019 ont été annoncés - tous les rapports ont été adoptés.

Cinq résolutions ont été adoptées le 15 octobre 2020 :

- Résolution sur la technologie de reconnaissance faciale ;
- Résolution sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise ;
- Résolution sur la responsabilisation dans le développement et l'utilisation de l'intelligence artificielle ;
- Résolution sur les défis en matière de protection des données personnelles et de la vie privée dans le contexte de la pandémie de COVID-19 ;
- Résolution sur les déclarations conjointes sur les questions internationales émergentes.

OCDE : Groupe de travail «Data Governance and Privacy in the Digital Economy»

Les travaux de ce groupe de travail se sont poursuivis au cours de l'année sous revue, bien que la réunion de novembre 2020 n'ait pu se tenir que de manière virtuelle. Deux thématiques sont à mentionner en particulier : d'une part, la « portabilité des données », à propos de laquelle le Secrétariat a présenté un projet de rapport et, de l'autre, le rapport du Secrétariat sur la mise en œuvre des « Lignes directrices de l'OCDE sur la protection de la vie privée ».

Brexit – Adéquation du niveau de protection des données

Le Royaume-Uni reste sur la liste des pays dont la législation assure un niveau de protection adéquat par rapport à la loi suisse sur la protection des données. Inversement, le Royaume-Uni reconnaît également la Suisse comme pays offrant une protection des données équivalente.

Comme déjà indiqué dans le dernier rapport d'activités (cf. 27e rapport, ch. 1.9), le Royaume-Uni s'est retiré de l'UE (Brexit) le 1er février 2020 après quelques atermoiements. La question de l'adéquation mutuelle s'est alors posée. Le Préposé a mené à ce propos de nombreux entretiens avec les autorités fédérales et les représentants du Royaume-Uni. Ces entretiens se sont poursuivis sur une base régulière pendant l'exercice en cours. En parallèle, des discussions ont eu lieu avec des représentants de la Commission de l'UE, car pendant longtemps rien n'indiquait clairement si l'UE allait encore accorder au Royaume-Uni le statut d'adéquation à partir de 2021. En revanche, le Royaume-Uni a reconnu comme équivalents au niveau légal tous les pays qui étaient également reconnus comme équivalents par l'UE au 31 décembre 2020.

Mais, étant donné que fin 2020 la décision de la Commission à propos de la Suisse était toujours en suspens, cela signifiait également que la Suisse restait reconnue par l'UE à cette date - et de ce fait serait automatiquement reconnue par la législation du Royaume-Uni, vraisemblablement pour les quatre années suivantes. Cela ne signifiait néanmoins pas que la Suisse accorderait automatiquement la réciprocité. Or la loi sur la protection des données au Royaume-Uni n'a pas changé de manière significative au cours de la période sous revue, de sorte que ce pays reste sur la liste des États dont la législation assure une protection adéquate des données en vertu de l'art. 6, al.1, LPD. Toutefois, un réexamen est réservé et dépend de l'orientation que prendra à l'avenir le droit sur la protection des données du Royaume-Uni.

Groupe de travail sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise

A l'occasion de la 42e Assemblée mondiale pour la protection de la vie privée (AMVP), le PFPDT a présenté une résolution sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise. Grâce au soutien de 15 autorités de protection des données, elle a été adoptée à l'unanimité.
Cette résolution vise à définir la position des membres de l'AMVP sur plusieurs des objectifs énoncés dans sa stratégie politique – plus précisément sur ceux qui concernent la progression de la protection de la vie privée à l'échelle mondiale et le renforcement des relations avec d'autres organismes et réseaux internationaux qui font progresser les questions de protection des données et de la vie privée.

Suite à l'adoption de cette résolution, il a été décidé de mettre en place un groupe de travail sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise. Ce dernier s'est fixé deux objectifs principaux :

- Répondre à la demande de coopération des acteurs pertinents afin de développer des lignes directrices et échanger les meilleures pratiques en matière de protection des données personnelles et de la vie privée tout en prenant en compte les spécificités de l'aide internationale au développement et de l'action humanitaire internationale ainsi que le besoin de faciliter leurs activités.
- Développer une stratégie de plaidoyer et de mobilisation auprès des acteurs pertinents.

Ce groupe de travail est coordonné par le PFPDT. Il rassemble des autorités de protection des données du monde entier ainsi que le CICR et l'Organisation internationale pour les migrations.

Règlement européen sur la protection des données

Le nouveau Règlement européen sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018. Sous certaines conditions, il est également applicable aux traitements de données par les entreprises de pays tiers. Les autorités de protection des données d'Albanie, de Jersey et de Monaco se sont réunies en Suisse pour discuter de nombreuses questions qui restent ouvertes.
Adopté le 27 avril 2016, le Règlement général sur la protection des données (RGPD) est applicable directement dans tous les États membres de l'Union européenne (UE) depuis le 25 mai 2018. Son champ d'application est toutefois bien plus vaste que le seul territoire de l'Union européenne. En effet, dès lors qu'il propose des biens ou des services à des personnes se trouvant au sein de l'Union européenne, ou qu'il observe le comportement desdites personnes notamment pour analyser leurs préférences, le responsable de traitement (ou le sous-traitant) est soumis aux exigences du RGPD, même s'il n'est pas établi dans l'UE. Les autorités francophones européennes non membres de l'Union européenne sont confrontées aux mêmes défis. Après une première réunion fructueuse à Monaco en 2018, le PFPDT a organisé une rencontre à Berne en février 2020 afin de permettre aux autorités d'échanger

sur l'entrée en vigueur du RGPD, de partager leurs expériences et mettre en commun les questions qui leur ont été adressées afin de coordonner leurs réponses.

Un peu plus d'un an après l'entrée en vigueur du RGPD, le Comité européen de la protection des données (CEPD), l'organe européen indépendant contribuant à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne, a publié ses lignes directrices sur le champ d'application du RGPD. Celles-ci avaient fait auparavant l'objet d'une consultation publique à laquelle le PFPDT avait participé en collaboration avec l'autorité monégasque de protection des données (CCIN - Commission de contrôle des informations nominatives) afin de demander la clarification d'un certain nombre d'éléments sur cette question hautement importante pour les pays tiers intégrés au paysage de l'UE. Cette dernière version a également été analysée et discutée lors de cette rencontre. Force est de constater qu'un certain nombre de questions restent encore ouvertes.

Groupes de coordination chargés de la surveillance des systèmes d'information SIS II, VIS et Eurodac

Au cours de l'année sous revue, les groupes de coordination de contrôle (GCC) ont tenu leurs deux réunions par visioconférence. Les discussions ont notamment porté sur les difficultés à trouver suffisamment d'experts au sein des autorités nationales de protection des données pour les évaluations Schengen.

Cette année encore, le Préposé, en tant qu'autorité nationale de surveillance, a participé aux réunions des trois GCC des systèmes d'information de l'UE, à savoir SIS II, VIS (présidence assurée par le Préposé) et Eurodac. Ces réunions ont eu lieu les 17 et 18 juin 2020 et les 25 et 26 novembre 2020 par visioconférence. Elles ont rassemblé le Contrôleur européen de la protection des données (CEPD) et les autorités nationales de protection des données des États membres.

Les GCC du SIS et du VIS se sont notamment penchés sur les causes des difficultés à rassembler suffisamment d'experts parmi les différentes autorités de protection des données en vue de l'évaluation Schengen de la protection des données, effectuée par la Commission européenne. Cette dernière, qui réexamine actuellement la procédure des évaluations de Schengen, a organisé une visioconférence sur ce sujet en janvier 2021 avec les autorités de protection des données des États Schengen et le CEPD. Cette conférence a permis un échange constructif sur les causes de ces difficultés et les possibilités d'y remédier. Les deux parties examineront l'éventualité de créer un pool d'experts pour la protection des données, chargé des évaluations Schengen. En outre, la Commission européenne mettra en place, dans la mesure du possible, une formation complémentaire pour les futurs experts chargés d'évaluer la protection des données. Lors de sa réunion du 18 juin 2020, le GCC VIS a confirmé la représentante du Préposé au poste de présidente du groupe de coordination pour une nouvelle période de deux ans.

Principe de la transparence

2.1 Généralités

La pandémie de COVID-19 n'est pas restée sans effet sur l'application du principe de la transparence dans l'administration fédérale. Elle a généré de la part des médias et de la société une forte demande d'informations transparentes et spécifiques sur les documents traitant du coronavirus. Certaines autorités ont ainsi reçu non seulement un grand nombre de demandes d'accès, mais aussi des demandes volumineuses et complexes, dont beaucoup nécessitaient une coordination entre offices, voire entre départements. Les événements ont montré qu'il peut être difficile et exigeant d'appliquer le principe de la transparence en période de pandémie. Alors que l'administration, soumise à des délais très courts, doit répondre aux attentes élevées du public avant d'en essuyer les critiques, les demandeurs exigent un accès rapide et complet afin de comprendre l'action de l'État pour lutter contre la pandémie, dont certains aspects découlent de mesures d'urgence. Cela dit, les statistiques indiquent que les autorités fédérales ont réussi, dans la majorité des cas, à appliquer le principe de la transparence dans l'administration fédérale, malgré l'urgence qui a caractérisé la gestion des affaires courantes pendant la pandémie.

Les chiffres ci-après (cf. ch. 2.2) révèlent par ailleurs que les tendances constatées ces dernières années (augmentation constante des demandes d'accès et forte proportion de cas dans lesquels un accès complet a été accordé) se sont confirmées en 2020.

La primauté de la médiation orale instaurée par le Préposé en 2017 a une nouvelle fois fait ses preuves pendant l'année sous revue. Si cela ne ressort pas clairement des chiffres à première vue, c'est à cause des ajustements qui ont dû être apportés à la procédure de médiation en raison de la pandémie. Lors de sa séance du 16 mars 2020, le Conseil fédéral a décidé, au vu de l'accélération de la propagation du coronavirus, de rendre obligatoire le télétravail et d'interdire les rassemblements de plus de cinq personnes. Le Préposé s'est alors vu contraint, afin de protéger la santé publique en général et celle des participants, de renoncer à ses séances de médiation pendant la première vague de la pandémie (de mars à juin 2020), puis également durant la seconde.

Pour toutes ces raisons, il a fallu, dans de nombreux cas, mener la procédure de médiation par écrit, avec deux conséquences : une diminution de la proportion de solutions amiables, et un allongement de la durée de traitement, d'où un encombrement de procédures. Les effets négatifs du recours au procédure de médiation écrite sur la durée de traitement et sur le résultat de la procédure seront exposés au ch. 2.3.

Le délai légal de 30 jours fixé pour les procédures de médiation est difficile à tenir, et pas seulement en période de pandémie. L'expérience montre qu'il est fréquemment dépassé dans les procédures complexes impliquant trois parties ou plus et portant sur des demandes d'accès à des documents relevant du secret d'affaires ou de la protection de la personnalité de particuliers. La procédure de médiation suppose que les autorités transmettent au Préposé les documents sollicités par les demandeurs, étant bien entendu que le Préposé est soumis au même secret de fonction que les autorités en question. En pratique, elles effectuent généralement cette transmission sans difficultés. Mais la collaboration ne se déroule pas toujours de manière optimale, comme l'illustre un cas particulier où il était question de l'obligation de collaborer à la médiation. En vertu du principe de la transparence dans l'administration instauré par la loi sur la transparence (LTrans; RS 152.3), les autorités ne sont plus libres de décider de l'opportunité de rendre ou non accessibles des informations et des documents officiels. Elles sont légalement obligées de collaborer à la médiation et de transmettre au Préposé tous les documents faisant l'objet d'une demande. Dans le cas particulier, l'autorité avait refusé de remettre les documents au Préposé, au motif que (de son point de vue) ils n'entraient pas dans le champ d'application de la

loi sur la transparence. De ce fait, le Préposé s'est vu dans l'impossibilité d'évaluer la qualité du document au sens de l'art. 5 LTrans et d'apprécier l'existence, invoquée par l'autorité, des motifs d'exceptions et de non-entrée en matière. Il s'est par conséquent vu obligé de recommander l'octroi d'un accès intégral aux documents demandés, car l'autorité chargée d'apporter la preuve doit porter le préjudice si elle n'est pas disposée à réfuter la présomption légale de l'accès aux documents officiels en les communiquant à l'autorité de médiation (cf. recommandation du 28 janvier 2021 [en allemand]).

On constate que d'année en année, l'administration s'efforce de restreindre l'application du principe de la transparence en introduisant des dérogations dans de nouvelles dispositions légales. En 2020, ce fut le cas dans la loi sur les cautionnements solidaires liés au COVID-19 (LCaS-COVID-19; RS 951.26; cf. ch. 2.4).

2.2 Demandes d'accès – Nouvelle hausse en 2020

Selon les chiffres qu'elles ont communiqués, les autorités fédérales ont reçu entre le 1er janvier et le 31 décembre 2020 1193 demandes d'accès contre 916 en 2019, ce qui correspond à une augmentation de 30 % sur un an. Ce chiffre inclut les demandes adressées au Ministère public de la Confédération (13) et aux Services du Parlement (6).

L'une des raisons de cette augmentation tient au besoin marqué de faire comprendre l'action de l'État dans la lutte contre la pandémie de COVID-19. Sur ces 1193 demandes, 308 (26 %) avaient un rapport avec le coronavirus. Les autorités ont établi une statistique des demandes d'accès en relation avec la pandémie (cf. ch. 3.3), qui montre que, par rapport à la statistique globale (cf. ci-dessous), l'accès complet a été accordé moins souvent (dans 121 cas, soit 39 %), et refusé intégralement à peine plus souvent (dans 38 cas, soit 12 %).

L'augmentation des demandes d'accès tient probablement aussi à ce qu'avec le temps, grâce notamment aux médias, la population est de mieux en mieux informée sur la loi sur la transparence et en exploite davantage les possibilités. Le Préposé table sur la poursuite de cette tendance au cours des années à venir.

Les autorités ont accordé un accès intégral aux documents dans 610 cas (51 %), contre 542 (59 %) l'année précédente, et un accès limité ou différé dans 293 cas (25 %). Elles ont refusé l'accès dans 108 cas (9 %). Par ailleurs, 35 demandes (3 %) ont été retirées, 80 étaient pendantes à la fin 2020, et 67 ne correspondaient à aucun document officiel. Depuis 2015, l'accès complet est accordé dans plus de 50 % des cas. Les refus sont clairement minoritaires et stagnent aux alentours de 10 %.

Par rapport aux années précédentes, on constate qu'en 2020, année du COVID, la proportion d'accès intégraux accordés a diminué de 8 % tandis que celle des accès partiels ou différés a augmenté de 6 %. Cette évolution s'explique en partie par le fait que les autorités ont, s'agissant des demandes concernant des documents «COVID» (soit un quart des demandes, comme on l'a vu plus haut), accordé moins souvent l'accès intégral, et plus souvent un accès limité ou différé, et qu'elles ont rejeté davantage de demandes.

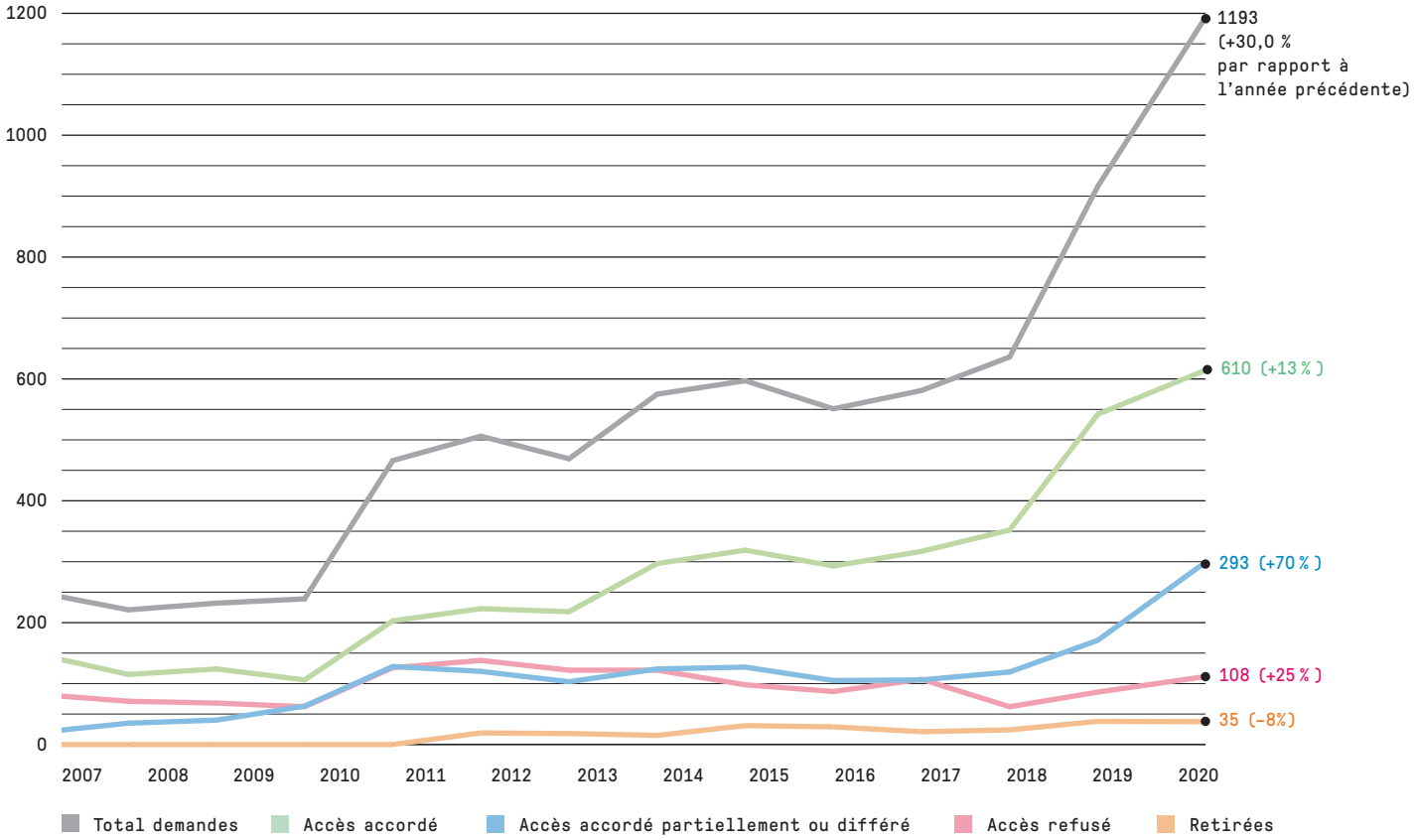
Départements et office fédéraux

En 2020, la pandémie de COVID-19 a focalisé l'attention des médias et de la société sur certaines unités administratives. Du fait de leurs tâches, l'OFSP, le DDPS et le DFF, notamment, ont été confrontés à un grand nombre de demandes. Selon ces autorités, il s'agissait en partie de demandes très volumineuses et complexes. Bien des cas ont exigé une coordination lourde entre offices ou entre départements, par exemple pour les documents relatifs à l'acquisition de biens médicaux. Le traitement a représenté pour ces autorités une charge de travail accrue par rapport aux années précédentes, pour des raisons évidentes.

À l'échelon des offices, c'est l'OFSP qui a signalé le plus de demandes (181) en 2020, dont 134 concernaient des documents «COVID» (cf. ch. 3.3). Viennent ensuite l'OFSPO (150), swissmedic (42) et l'OFEV (38). À l'échelon des départements, le DFI (312) et le DDPS (251) sont en tête. À l'inverse, 13 autorités déclarent n'avoir reçu aucune demande d'accès en 2020. Le Préposé lui-même en a reçu dix, dont huit auxquelles l'accès a été complètement accordé. Une des demandes ne correspondait à aucun document et la dernière était encore pendante à la fin de l'année.

En 2020, les émoluments perçus pour l'accès à des documents officiels ont atteint un montant de 15 189 francs, inférieur à celui de l'année précé-

Graphique 1 : Demandes d'accès – évolution depuis 2006



dente. (18 185 francs). Un montant total de 450 francs été exigé pour deux demandes d'accès à des documents «COVID».

Alors que le DFJP et la Chancellerie fédérale n'ont pas prélevé d'émoluments, les six autres départements ont facturé aux demandeurs d'accès une partie du temps consacré au traitement (DFI: 4643 francs; DEFR: 3786 francs; DETEC: 3310 francs; DFF: 1900 francs; DFAE: 900 francs; DDPS: 650 francs). Signalons que 25 seulement des 1193 demandes déposées ont donné lieu à la perception d'émoluments, contre 31 l'année précédente, ce qui représente une nette diminution tant du nombre de cas concernés que du montant total des émoluments. C'est d'autant plus remarquable que le nombre des demandes a (une nouvelle fois) sensiblement augmenté. Comme les années précédentes, la perception d'émoluments reste une exception: près de 98 % des demandes d'accès y échappent. La pratique de l'administration conforte donc le principe de la gratuité de l'accès aux documents officiels proposé par la Commission des institutions politiques du Conseil national (cf. ch. 2.4, Avis du PFPDT).

S'agissant du temps consacré au traitement des demandes d'accès, le Préposé rappelle que les autorités ne sont pas tenues de le consigner et qu'il n'existe pas de directive de saisie uniforme pour l'ensemble de l'administration fédérale. Aussi les indications qui lui sont fournies (volontairement) ne reflètent-elles que partiellement la réalité. Selon ces données, le temps consacré au traitement est passé de 4375 heures en 2019 à 5010 heures en 2020. Cette augmentation de 15 % est modérée par rapport à celle du nombre des demandes (30 %). Le temps consacré à la préparation des procédures de médiation a lui aussi augmenté: les autorités font état de 569 heures (contre 473 en 2019).

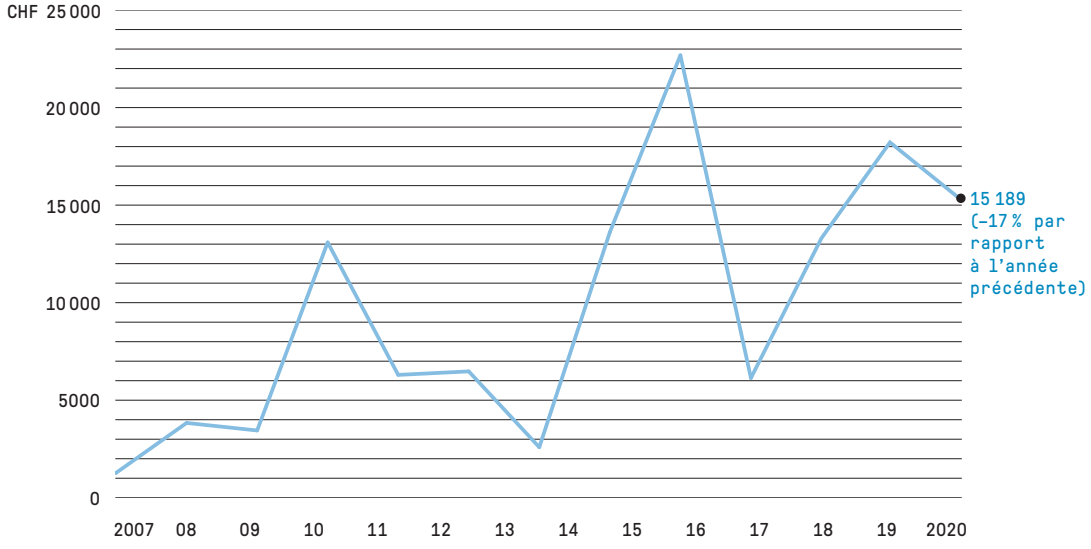
Services du Parlement

Les Services du Parlement ont déclaré avoir reçu six demandes d'accès, qui ont toutes été rejetées à l'exception d'une seule, qui ne correspondait à aucun document officiel.

Ministère public de la Confédération

Le Ministère public de la Confédération a déclaré avoir reçu en 2020 13 demandes. Il a accordé l'accès dans six cas et l'a refusé dans un. Sur les six demandes restantes, deux ne correspondaient à aucun document officiel, et quatre étaient encore pendantes à la fin de l'année sous revue.

Graphique 2 : Émoluments prélevés depuis l'entrée en vigueur de la LTrans



2.3 Procédures de médiation – Une demande en baisse

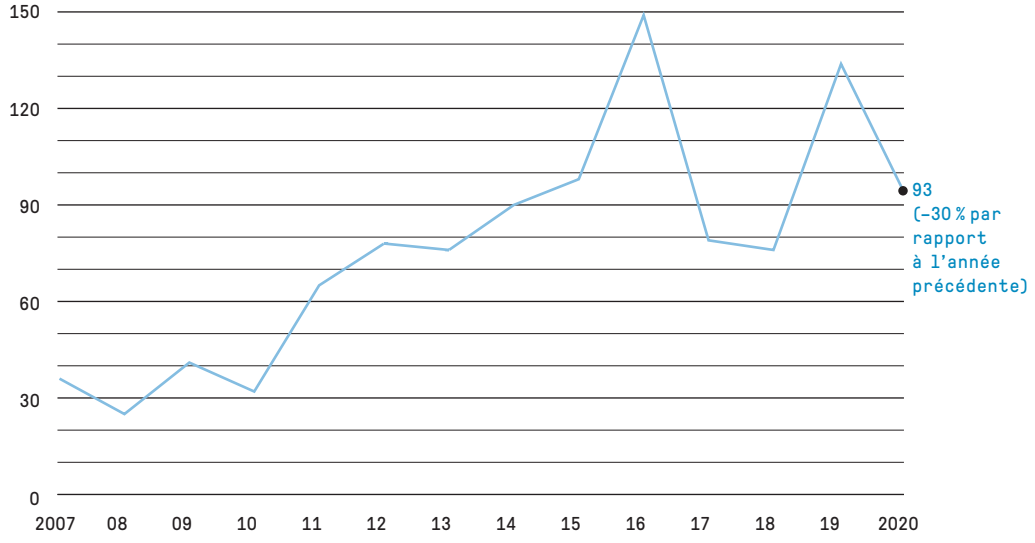
En 2020, le Préposé a reçu 93 demandes en médiation, ce qui correspond à une baisse de 30 % par rapport aux 133 demandes reçues en 2019 (dont 28 portaient sur le même état de fait). La plupart des demandes émanaient de particuliers (42) et de journalistes (31). Ces chiffres appellent le constat suivant: sur les 401 demandes rejetées en partie ou intégralement par l'administration fédérale, 93 (soit 23 %) ont donné lieu à une demande en médiation auprès du Préposé, dont 24 (26 %) concernaient des documents officiels liés au coronavirus.

Le Préposé a traité 119 demandes en médiation en 2020, dont 79 avaient été déposées cette année-là, et 40 l'année précédente. Les parties ont trouvé un accord dans 40 cas. Le Préposé a en outre émis 27 recommandations, qui ont permis de régler 55 cas dans lesquels aucun accord n'était envisageable.

Aux cas réglés s'ajoutent onze demandes remises hors délai, douze pour lesquelles les conditions d'application de la loi sur la transparence n'étaient pas remplies, une qui a été retirée.

À la fin de l'année, huit procédures de médiation ont été suspendues en accord avec les parties.

Graphique 3: Demandes en médiation depuis l'entrée en vigueur de la LTrans



Proportion des solutions amiables

Le recours aux séances de médiation présente de nombreux avantages, dont ceux d'accélérer la procédure d'accès aux documents et de jeter les bases d'une éventuelle collaboration future entre les personnes impliquées dans la séance de médiation. L'efficacité des mesures instaurées en 2017 et des séances de médiation se perçoit régulièrement dans la proportion de solutions amiables par rapport aux recommandations.

Au cours de l'année sous revue, 40 solutions amiables ont été trouvées, et le Préposé a émis 27 recommandations afin de régler 55 cas. Les solutions amiables ne représentent donc que 34 % des procédures de médiation, ce qui est nettement moins que l'année précédente (cf. tableau 1).

Comme relevé au ch. 2.1, la pandémie de COVID-19 a contraint le préposé de renoncer aux séances de médiation du mois de mars au mois de juin 2020, soit dans 13 cas. Pour aboutir à une solution amiable, il faut que la procédure de médiation ait lieu. Sur les 40 procédures menées en 2020, 24 (60 %) ont abouti à un accord, ce qui correspond aux chiffres des années précédentes.

L'augmentation apparente, en comparaison aux années précédentes, du nombre de procédures de médiation ayant donné lieu à une recommandation s'explique essentiellement par une anomalie statistique: dans deux cas, un nombre inhabituellement élevé de tiers concernés a déposé une demande en médiation (dix dans le premier cas, 18 dans le second). Ces 28 demandes ont produit plus de la moitié des cas réglés par une recommandation.
Le Préposé constate l'efficacité constante des médiations orales pour l'émergence de solutions rapides et consensuelles. Dans certains cas, les participants ont demandé, compte tenu des mesures «COVID», une suspension de la procédure jusqu'au moment où les négociations orales seront de nouveau possibles.

Le Préposé publie toutes ses recommandations sur son site Internet.

Tableau 1 : Solutions amiables

2020	**34 %**
2019	61 %
2018	55 %

Durée des procédures

Le tableau 2 est divisé en quatre colonnes en fonction de la durée de traitement. Précisons que la durée pendant laquelle une procédure est suspendue à la demande des parties ou en accord avec elles n'est pas prise en compte. Il peut y avoir suspension, notamment, lorsqu'une autorité souhaite revoir sa position à l'issue d'une séance, ou lorsqu'elle doit procéder à l'audition de tiers concernés. Si la séance est reportée à la demande d'une des parties (pour cause de vacances, de maladie, etc.), la période qui s'étend entre le délai initialement prévu et le nouveau n'est pas non plus prise en compte.

Le tableau 2 montre que 43 % des procédures réglées en 2020 l'ont été dans le délai réglementaire de 30 jours, 30 % dans un délai compris entre 31 et 99 jours, et 27 % en 100 jours ou davantage.

Les principaux motifs de dépassement du délai sont l'absence des personnes ou des autorités concernées (vacances, maladie, voyage), l'implication d'un grand nombre de tiers ou la complexité juridique du cas à traiter, auxquels s'est ajouté durant l'année sous revue l'empêchement, pour cause de COVID-19, des parties ou du personnel du Préposé. Ces motifs concernent les 32 cas dont le traitement a duré 100 jours ou plus, étant précisé que l'un a regroupé dix procédures, et un second 18. Parmi les motifs de dépassement figurent aussi les consultations menées à l'étranger, les efforts des parties pour parvenir à négocier, l'abondance des documents ou encore le grand nombre des personnes concernées. Le traitement de ces cas nécessitant fréquemment un surcroît important de travail, le Préposé peut, en vertu de l'art. 12a de l'ordonnance sur le principe de la transparence dans l'administration (OTrans; RS 152.31), prolonger d'une durée raisonnable le délai réglementaire. Pendant l'année sous revue, certaines autorités particulièrement éprouvées

Tableau 2 : Durée de traitement des procédures de médiation

Durée du traitement en jours	Période 2014 – août 2016*	Phase pilote 2017	Période 2018	Période 2019	Période 2020
dans un délai de 30 jours	11 %	59 %	50 %	57 %	43 %
de 31 à 99 jours	45 %	37 %	50 %	38 %	30 %
plus de 100 jours	44 %	4 %	0 %	5 %	27 %

*Source : présentation du Préposé, rencontre organisée pour les dix ans de la LTrans le 2 septembre 2016

par la pandémie de COVID-19 se sont vu accorder un allongement des délais de traitement.

Les 30 jours du délai légal de traitement des procédures de médiation sont généralement respectés lorsque les séances se déroulent selon l'échéancier prévu, sans demande de report de la part des parties, et s'achèvent par un accord. Lorsqu'aucun accord n'est trouvé, le Préposé n'est pas toujours en mesure d'émettre sa recommandation écrite dans les 30 jours qui suivent la réception de la demande.

L'augmentation de la proportion de procédures écrites et de recommandations écrites due à la pandémie a généré pour le Préposé un surcroît de travail considérable, avec à la clé un allongement des délais de traitement et donc des retards. Compte tenu du nouveau confinement décidé début 2021, le Préposé doit s'attendre à une aggravation de ces retards.
Par ailleurs, il est encore arrivé pendant l'année sous revue que des tiers consultés fassent appel à un avocat dès le stade de la procédure d'accès et de médiation, démarche peu propice à l'obtention d'une solution simple, rapide et pragmatique.

Nombre de cas pendants

Les chiffres ci-dessous indiquent le nombre de cas pendants à la fin de chaque année. Début janvier 2021, il y avait 17 procédures pendantes, dont huit (trois datant de 2019 et cinq de 2020) suspendues. Le Préposé en a terminé sept avant la mise sous presse du présent rapport.

Tableau 3: Procédures de médiation pendantes

Fin 2020	**17 (dont 9 terminées à la mise sous presse et 8 suspendues)**
Fin 2019	43 (dont 40 terminées à la mise sous presse et 3 suspendues)
Fin 2018	15 (dont 13 terminées en février 2019 et 2 suspendues)

2.4 Consultations des offices

CORONA

Processus législatif de transposition de l'ordonnance sur les cautionnements solidaires liés au COVID-19 dans la loi éponyme

La loi sur les cautionnements solidaires liés au COVID-19 (LCaS-COVID-19) prévoit que dans le cadre du programme de cautionnement de la Confédération, l'identité et les coordonnées bancaires des entreprises et des personnes et le montant des crédits alloués ou refusés ne puissent pas être rendus publics. Lors du processus législatif, le Préposé s'est opposé en vain contre cette limitation du principe de la transparence.

En adoptant, le 25 mars 2020, une ordonnance de nécessité à durée limitée, le Conseil fédéral a permis à de nombreuses entreprises d'accéder rapidement à un financement transitoire qui leur assure les liquidités nécessaires pour surmonter la crise liée à la pandémie. Le contenu de cette ordonnance a été transposé dans une loi fédérale urgente limitée dans le temps, que le Parlement a adoptée en décembre 2020.

L'art. 12, al. 2, LCaS-COVID-19 dispose que les données personnelles et informations relatives aux entreprises et aux personnes qui recherchent et prennent un crédit ne peuvent pas être rendues publiques si elles contiennent l'identité et les coordonnées bancaires de ces entreprises et de ces personnes, et les montants qui sont alloués ou refusés. Conformément au message relatif à la LCaS-COVID-19, il s'agit là d'une disposition spéciale au sens de l'art. 4 LTrans, ce qui exclut les informations en question du champ d'application de la LTrans et les rend par conséquent inaccessibles sur demande.

Le Préposé s'est déclaré contre cette disposition spéciale, tant lors de la consultation relative à la LCaS-COVID-19 que lors de la consultation des offices sur le message et le projet de loi qui a suivi, en rappelant que la LTrans avait notamment pour but d'assurer la traçabilité de l'action de l'administration et de prévenir la mauvaise gestion et la corruption. Étant donné que 40 milliards de francs d'argent public sont en jeu, rien ne justifiait selon lui le maintien inconditionnel du secret sur les informations en question. D'autant que si les crédits accordés généraient des pertes, il faudrait recourir à l'argent du contribuable pour les éponger. Compte tenu de la contestation qu'a suscitée ultérieurement l'action de l'administration en relation avec les cautionnements solidaires de la flotte de haute mer, le Préposé s'étonne de ce que le Parlement a inscrit le maintien du secret proposé par le Conseil fédéral dans la loi adoptée le 19 décembre 2020.

Le Préposé a souligné en vain, lors de la consultation, que les intérêts privés légitimes resteraient protégés même si la LTrans s'appliquait. Celle-ci protège en effet expressément les secrets d'affaires (art. 7, al. 1, let. g, LTrans), la sphère privée et les données personnelles des personnes physiques et des personnes morales (art. 7, al. 2, et 9, al. 2, LTrans, et art. 19 LPD). Le Préposé a aussi rappelé que selon la doctrine et la jurisprudence, le secret bancaire prime sur la LTrans. Dans son avis, il a renvoyé tout aussi vainement à la loi fédérale sur les aides financières et les indemnités (loi sur les subventions, RS 616.1) et à la loi fédérale sur les aides financières aux organisations de cautionnement en faveur des PME (RS 951.25). Bien que ces deux lois présentent des points communs évidents avec la LCaS-COVID-19, elles ne prévoient pas de dispositions spéciales au sens de l'art. 4 LTrans.

Consultation des offices relative au projet d'avis du Conseil fédéral sur le rapport de la Commission des institutions politiques du Conseil national (CIP-N) du 15 octobre 2020 relatif à l'initiative parlementaire Graf-Litscher 16.432 « Principe de la transparence dans l'administration. Faire prévaloir la gratuité de l'accès aux documents officiels ».

La CIP-N a rédigé un projet de loi érigeant en principe la gratuité de l'accès aux documents officiels, la possibilité de percevoir des émoluments étant limitée à certaines exceptions. Le Conseil fédéral souhaite pouvoir fixer lui-même, dans l'ordonnance, le montant maximal des émoluments. Le Préposé préférerait, lui, que ce plafond soit inscrit directement dans la LTrans.

L'initiative parlementaire 16.432 « Principe de la transparence dans l'administration. Faire prévaloir la gratuité de l'accès aux documents officiels » vise à modifier la LTrans de façon à rendre l'accès aux documents officiels libre d'émoluments.

La CIP-N, compétente pour cet objet, a adopté un avant-projet de modification de la LTrans, qu'elle a remanié à l'issue de la consultation à l'intention de son conseil. Le but est d'inscrire dans la LTrans le principe de la gratuité de l'accès aux documents officiels. La possibilité pour l'autorité de percevoir des émoluments doit être réservée à des cas exceptionnels, « lorsque la demande d'accès nécessite un surcroît important de travail de sa part ». La majorité de la commission estime qu'il faut plafonner les émoluments à 2000 francs dans la LTrans, le Conseil fédéral réglant les détails et le tarif en fonction du travail nécessaire. Une minorité considère que c'est aussi au Conseil fédéral de fixer le plafond.

Le Préposé soutient la proposition de la majorité de la commission consistant à fixer directement le plafond des émoluments dans la LTrans, car cela permet de garantir au niveau de la loi que la perception exceptionnelle d'émoluments ne prendra pas des proportions revenant à entraver l'accès aux documents officiels. Le Conseil fédéral s'étant prononcé contre l'inscription du plafond dans la loi, c'est à présent au Conseil national de donner son avis.

Révision de la loi fédérale sur l'encouragement de la recherche et de l'innovation (LERI). Consultation des offices dans le cadre des travaux préparatoires du message du Conseil fédéral

Lors de la consultation relative à la révision de la LERI, un durcissement de la règle relative à la communication des noms des rapporteurs et des experts scientifiques dans les procédures de recours a été demandé. Le Préposé s'est déclaré contre cette proposition.

En cas de recours pour non-octroi de contributions à la recherche, l'art. 13, al. 4, LERI prévoit que « les noms des rapporteurs et des experts scientifiques ne peuvent être communiqués au recourant qu'avec leur accord ». Le Tribunal administratif fédéral (TAF), dans son arrêt A-6160/2018 du 4 novembre 2019 relatif à un recours fondé sur la LTrans, a donné de l'art. 13, al. 4, LERI l'interprétation suivante : les noms en question peuvent être communiqués à des tiers non impliqués dans la procédure si les rapporteurs et les experts scientifiques concernés y ont expressément consenti. Il a précisé qu'il s'agit d'une disposition spéciale au sens de l'art. 4 LTrans, ce qui fait que la LTrans ne s'applique pas, tout en estimant que

l'art. 13, al. 4, LERI ne constitue pas une obligation générale de garder le secret.

Dans le cadre de la consultation relative à la révision de la LERI, le Fonds national suisse a proposé de restreindre la règle relative à la communication des noms de telle sorte que seuls les recourants puissent demander cette communication.
Par la suite, le Préposé a combattu avec succès l'intégration de cette proposition dans le projet devant le Secrétariat d'État à la formation, à la recherche et à l'innovation, qui dirige les travaux.

La proposition ne figure pas dans le message du Conseil fédéral du 17 février 2021.

Révision partielle de la loi fédérale sur l'assurance-maladie (LAMal) concernant les mesures visant à maîtriser les coûts (second volet)

L'Office fédéral de la santé publique (OFSP) élabore une révision partielle de la LAMal concernant les mesures visant à maîtriser les coûts. Ce projet prévoit notamment d'exclure du principe de la transparence tous les documents liés aux modèles de prix des médicaments dans l'assurance maladie. Le Préposé est opposé à ce projet.

Dans le 27e rapport d'activités 2019/2020, le Préposé évoquait l'ouverture prochaine de la consultation relative à une révision partielle de la LAMal, laquelle a eu lieu au cours de l'année sous revue. Le Préposé s'est déclaré contre le projet de l'OFSP visant à supprimer le droit du public de consulter les documents relatifs à la détermination du prix des médicaments. Il estime que le prix effectif des médicaments pris en charge par l'assurance obligatoire des soins et les documents servant à la fixation de ce prix doivent rester accessibles au public, sous peine de voir émerger une pratique opaque quant aux critères de vérification et d'admission dans la liste des spécialités et quant au mécanisme de remboursement. Il est essentiel selon lui que la population et les entreprises concurrentes conservent la possibilité de comprendre et de vérifier entièrement la pratique d'autorisation de l'OFSP. Le résultat de la consultation n'est pas encore connu à l'heure où nous mettons sous presse.

Au cours de l'année sous revue, le Préposé a mené une procédure de médiation à propos de documents de l'OFSP relatifs à la fixation de prix de médicaments dans l'assurance maladie obligatoire. Le demandeur sollicitait l'accès à des informations concernant des médicaments assortis d'un modèle de prix. La médiation n'ayant abouti à aucun accord entre l'OFSP et le demandeur, le Préposé a dû émettre une recommandation écrite. Pour justifier son refus de communiquer les documents demandés, l'OFSP a principalement invoqué l'argument selon lequel seul le maintien du secret permettait de garantir la sécurité de l'approvisionnement en médicaments innovants et coûteux. Le Préposé a notamment déclaré dans sa recommandation que selon lui, la LTrans en vigueur ne permettait aucunement d'anticiper la modification législative visée par le Conseil fédéral. L'OFSP n'ayant par conséquent pu faire valoir aucun motif de dérogation en vertu de la LTrans ni réfuter la présomption légale de l'accessibilité aux informations demandées, le Préposé a recommandé l'accès intégral.

Nouvelle loi fédérale fixant le cadre général de la perception des redevances et concernant le contrôle de la circulation transfrontalière des marchandises et des personnes par l'Office fédéral de la douane et de la sécurité des frontières (LE-OFDF – loi définissant les tâches d'exécution de l'OFDF)

L'Administration fédérale des douanes (AFD) a ouvert au dernier trimestre 2020 la consultation relative à la création d'une loi définissant les tâches d'exécution du futur Office fédéral de la douane et de la sécurité des frontières (OFDF). Ce projet ne prévoit plus de restrictions du principe de la transparence.

Dans le 27e rapport d'activités 2019/2020, le Préposé faisait le point sur la consultation des offices concernant l'ouverture de la consultation relative au projet de loi fédérale sur la douane et la sécurité des frontières. Ce projet a été retravaillé à l'issue de la consultation des offices et renommé « loi fédérale fixant le cadre général de la perception des redevances et concernant le contrôle de la circulation transfrontalière des marchandises et des personnes par l'Office fédéral de la douane et de la sécurité des frontières » (loi définissant les tâches d'exécution de l'OFDF). L'AFD, prenant en considération les inquiétudes du Préposé, y a supprimé les restrictions initialement prévues du principe de la transparence. La consultation a eu lieu au cours de l'année sous revue.

Le PFPDT

3.1 Tâches et ressources

CORONA

Pandémie

La crise a généré la réalisation urgente de projets de traitement de données pour lutter contre la pandémie et gonflé la demande de documents officiels, ce qui a exigé un effort considérable de la part de l'ensemble du personnel.

En tant qu'unité administrativement subordonnée à la Chancellerie fédérale, le PFPDT a mis en œuvre toutes les prescriptions du Conseil fédéral visant à protéger le personnel contre le virus. Aussi ses collaborateurs ont-ils effectué une bonne partie de leur travail à distance pendant la période sous revue. Les rencontres entre personnes n'ont été possibles que pendant quelques rares semaines, ce qui a notamment compliqué l'intégration et le suivi des nouveaux collaborateurs.

Prestations et ressources dans le domaine de la protection des données

Effectif

De 2005 à 2019, l'effectif affecté à l'application de la loi fédérale sur la protection des données (LPD) a fluctué entre 20 et 24 équivalents plein temps. Ces fluctuations tiennent à deux motifs : d'une part, le Conseil fédéral n'ayant jamais approuvé les postes prévus pour l'application de la loi sur la transparence (LTrans) entrée en vigueur en 2006, le PFPDT a dû se rabattre sur le personnel existant avec le soutien occasionnel de la Chancellerie fédérale, d'autre part, les postes supplémentaires accordés dans le contexte de l'adhésion aux accords de Schengen et de Dublin et de l'édiction de lois spéciales dans le domaine de la santé n'ont jamais pu être entièrement pourvus en raison de mesures générales d'économie.

Dans son message concernant la révision totale de la LPD, le Conseil fédéral a prévu pour le Préposé la création de neuf à dix postes supplémentaires (FF 2017 6565 6784). Depuis lors, le législateur fédéral a anticipé un aspect partiel de cette révision totale avec la nouvelle loi fédérale sur la protection des données dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS, RS 235.3). Après avoir mis en vigueur cette loi le 1er mars 2019, le Conseil fédéral a attribué au Préposé trois postes supplémentaires pour la mise en œuvre des tâches et des compétences nouvelles. L'effectif est ainsi passé en 2020 à 27 équivalents plein temps. Au printemps 2021, le Préposé a demandé au Conseil fédéral la création des six postes à plein temps restants, dans la perspective de l'entrée en vigueur, prévue en 2022, de la LPD révisée.

Par suite de plusieurs départs, à la retraite notamment, la structure d'âge de l'autorité a baissé, ce qui a allégé ses charges de personnel.

Tableau 4: Postes pouvant être affectés aux questions relatives à la LPD

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27

Prestations

Conformément au nouveau modèle de gestion de l'administration fédérale (NMG), les tâches du PFPDT en tant qu'autorité de protection des données compétente pour les organes fédéraux et le secteur privé sont réparties entre les quatre groupes de prestations suivants : conseil, surveillance, information et législation. Au cours de l'année de référence allant du 1er avril 2020 au 31 mars 2021, les ressources en personnel dont dispose le Préposé pour la protection des données ont été affectées de la manière suivante :

Tableau 5 : Prestations en matière de protection des données

Conseil Privés	24,8 %	
Conseil Confédération	20,1 %	
Collaboration avec les cantons	1,8 %	
Collaboration avec des autorités étrangères	11,1 %	
Total conseil		**57,8 %**
Surveillance	15 %	
Certification	0,1 %	
Registre de données	0,4 %	
Total surveillance		**15 %**
Information	17 %	
Formation/Conférences	2,4 %	
Total information		**19,4 %**
Législation	7,3 %	
Total législation		**7,3 %**
Total protection des données		**100,0 %**

Conseil

Comme cela a été indiqué dans le chapitre introductif «Défis actuels», le Préposé est confronté à une demande constamment élevée de prestations de conseil en raison de la nécessité de suivre les projets numériques d'envergure. Les ressources en personnel consacrées au conseil ont augmenté de près de 7 %, pour atteindre 57,8 %. Selon le planning de contrôle du Préposé pour l'année 2021, le suivi de quinze grands projets est en cours. Six d'entre eux ont trait à la transformation numérique de l'administration fédérale ordonnée par le Conseil fédéral afin de rattraper le retard dénoncé par les politiques et les médias et dû notamment à la lutte contre la pandémie.

Ses ressources n'étant toujours pas adaptées aux risques juridiques et technologiques liés au dynamisme de la transformation numérique, le Préposé n'a pas pu, cette année encore, répondre dans la mesure et les délais souhaités à la demande croissante d'accompagnement de projets. Les trois équipes du domaine de direction Protection des données ont répondu chaque mois à une soixantaine de demandes et de signalements de citoyens par une lettre-type les réorientant vers les voies civiles. Cette situation entraîne une incompréhension croissante parce que d'une part, le Règlement général sur la protection des données de l'UE oblige les autorités locales de protection des données à donner suite à toutes les plaintes des citoyens, et d'autre part, la nouvelle LPD prévoit, pour le PFPDT aussi, une obligation élargie de traiter matériellement les requêtes individuelles de la population suisse.

Étant donné que le «big data» et l'intelligence artificielle s'imposent comme modèles économiques dans tous les secteurs et que les risques technologiques qui pèsent sur la protection des données élargissent encore le domaine de surveillance du PFPDT, on peut, comme les années précédentes, s'attendre à voir augmenter encore le nombre de grands projets de traitement de données dans l'administration et l'économie.

Tableau 6 : Activité de conseil sur des projets d'envergure en 2021

Droits fondamentaux	5
Finances	1
Santé et secteur du travail	3
Télécommunication	1
Commerce et économie	2
Archives fédérales	1
Migration	1
Douane	1
Total	**15**

Surveillance

Le dynamisme des applications fondées sur l'informatique en nuage (Cloud Computing) impose aujourd'hui une exécution rapide des contrôles. Cette accélération et la nécessité croissante d'allier compétences juridiques et techniques excluent toute interruption longue dans les procédures d'établissement des faits, si bien qu'il faut affecter aux contrôles d'envergure plusieurs collaborateurs. L'effectif actuel restreint considérablement la densité des contrôles. En 2018, les activités de surveillance ont mobilisé environ 12 % des ressources en personnel, ce qui est nettement inférieur à la moyenne d'environ 20 % établie sur plusieurs années. Au cours des dernières périodes de référence, le Préposé a au moins pu éviter que cette proportion ne descende au-dessous de 15 %. Selon le plan de contrôle 2021, ces ressources serviront à effectuer 13 contrôles approfondis. Par rapport au volume traité par les organes fédéraux et aux quelque 12 000 grandes et moyennes entreprises commerciales et 100 000 fondations et associations de Suisse, la densité actuelle des contrôles reste faible, et il est toujours difficile pour le Préposé de faire part aux médias et aux associations de protection des consommateurs de sa réticence, faute de ressources, à ouvrir des procédures d'établissement des faits. La perspective de l'entrée en vigueur de la nouvelle LDP a accru les attentes du public. Le Préposé espère que le Conseil fédéral en tiendra compte et qu'il lui accordera les six postes demandés.

Législation

La transformation numérique des offices fédéraux entraîne pour le traitement des données des changements qui ne sont admissibles que s'ils se fondent sur des bases légales. Il en résulte un grand nombre de nouvelles dispositions dans le droit fédéral, sur lesquelles le Préposé est appelé à se prononcer dans diverses procédures de consultation. Malgré la charge de travail que cela représente, sans parler de la révision de la LPD et de son ordonnance d'application, le Préposé est parvenu ces dernières années à stabiliser son activité de surveillance à un niveau bas en réservant notamment ses avis détaillés aux projets les plus importants.

Révision totale de la LPD

L'entrée en vigueur imminente de la nouvelle LPD et de son ordonnance d'application entraîne pour le Préposé un important travail préparatoire concernant ses tâches et ses compétences nouvelles et l'information en temps utile de la population et des acteurs économiques. La validation, par le Conseil fédéral, de trois postes à cet effet a contribué à faire avancer ces travaux.

Participation aux délibérations de commissions et auditions par les commissions parlementaires

La Commission des institutions politiques du Conseil national (CIP-N) a invité le Préposé à deux reprises en avril 2020 à propos d'une application de visualisation des rassemblements de personnes proposée par Swisscom dans le cadre des mesures anti-COVID-19. Elle l'a ensuite entendu début mai au sujet de l'instauration de l'application d'alerte SwissCovid. À la même période, la CIP du Conseil des États (CIP-E) a consulté le Préposé à propos de la révision de la LPD (élimination des divergences) et de la révision partielle de la loi sur l'AVS en relation avec l'utilisation du numéro AVS. Fin mai, elle l'a entendu à deux reprises à propos de la modification urgente de la loi sur les épidémies. Elle l'a par ailleurs consulté au sujet des révisions de la LPD et de la loi sur l'AVS, avant de l'inviter, en juillet 2020 à l'élimination des divergences concernant la révision de la LPD. En juillet toujours, les sous-commissions DFJP / ChF des Commissions de gestion (CdG) ont invité le Préposé à présenter son rapport d'activités annuel.

Au cours de l'exercice sous revue, le Préposé a par ailleurs été entendu par la CdG du Conseil national au sujet du dossier électronique du patient et par la CIP-E au sujet de la protection des données dans le milieu de la santé, lors de la session des jeunes.

Les CIP des deux chambres ont en outre invité le Préposé à cinq séances, les Commissions de la sécurité sociale et de la santé publique à deux séances,

consacrées à l'allégement des mesures pour les personnes vaccinées et à d'autres sujets liés au COVID-19.

Critères de calcul

C'est aux autorités politiques qu'il appartient de définir les ressources du PFPDT. Elles disposent, pour évaluer les développements actuels et futurs du numérique et leurs conséquences sur les activités de notre autorité, d'une marge de manoeuvre considérable. La tâche principale du Préposé consiste à protéger la sphère privée et à garantir le droit à l'autodétermination en matière d'information dans la société numérique. Il doit pouvoir agir en toute indépendance.

Cela nécessite des ressources humaines, matérielles, techniques et financières appropriées, qui ne limitent pas l'action du Préposé au strict nécessaire mais lui laissent au contraire l'initiative d'agir avec un degré de crédibilité et d'intensité que le public concerné peut raisonnablement attacher à la protection de ses droits fondamentaux.

Compte tenu de ces éléments, le Préposé a défini pour chaque groupe de prestations les objectifs ci-après, déterminants pour le calcul des ressources :

Prestations et ressources dans le domaine de la loi sur la transparence

Le domaine de direction Principe de la transparence, qui a employé pendant l'année sous revue 4,4 personnes, a adopté en 2017, à l'issue d'une période d'essai d'un an, une procédure accélérée et sommaire selon laquelle, en principe, les médiations sont désormais menées oralement. Cette procédure a fait ses preuves car la proportion de médiations abouties reste élevée année après année et le dépassement des délais légaux concerne presque uniquement des affaires complexes sur le plan tant de la procédure que du contenu.
Pendant l'année sous revue et cette année encore, la pandémie et les mesures de santé publique prises par le Conseil fédéral ont empêché la tenue de médiations orales, obligeant le préposé à repasser à la procédure écrite. La durée de traitement en a immédiatement pâti, et le nombre de demandes (complexes) ne diminuant pas, il en en résulté des retards. Par ailleurs, on a vu une fois de plus au cours de l'année sous revue que la multiplication rapide des demandes en médiation alliée aux postes vacants entraînent rapidement des retards, au détriment du respect des délais légaux (cf. ch. 2.2).

Comme la hausse du nombre de demandes devrait se poursuivre en 2021, la situation a peu de chances de s'arranger si l'effectif n'augmente pas.

Tableau 7 : Critères de calculs PFPDT

Groupes de prestations	Objectifs de résultats
Conseil	Le PFPDT développe une présence pour des conseils adaptés aux attentes des particuliers ainsi que le soutien à des projets portant sur des données personnelles sensibles de l'économie et des autorités fédérales à l'aide d'instruments de travail adaptés à la numérisation.
Surveillance	Le PFPDT développe une densité plausible de contrôles.
Information	Le PFPDT sensibilise de manière proactive le public aux risques technologiques et empiriques de la numérisation.
Législation	Le PFPDT exerce une influence rapide et active sur toutes les normes et réglementations spéciales relatives à la protection des données qui sont élaborées tant au niveau national qu'international. Elle aide les parties intéressées à formuler des bonnes pratiques.


OPEN
RIDE

3.2 Communication

La pandémie, sujet dominant

L'année sous revue a commencé à peu près au moment où déferlait sur la Suisse la pandémie de COVID-19. Ce sujet a marqué l'année tout entière, et n'a pas fini de faire sentir ses effets. Le Préposé a focalisé sa communication sur l'identification et sur la publication des risques pour la protection des données. Bien qu'il soit en principe indépendant, il a dû, à maintes reprises, se concerter avec d'autres autorités afin de garantir la cohérence des informations livrées à la population pendant la crise. Ce fut notamment le cas avec les responsables cantonaux de la protection des données.

Au-delà de la pandémie, l'accélération de la transformation numérique et de la mondialisation de la société a elle aussi fait de la protection des données un sujet omniprésent. Le Préposé a donc dû effectuer un important travail dans de nombreux domaines pour sensibiliser efficacement les journalistes et le grand public aux questions urgentes relatives à la protection de la sphère privée et au principe de la transparence dans l'administration.

Il a par ailleurs accompagné le débat parlementaire sur la révision totale de la protection des données (LPD), qui a pris fin avec l'adoption du projet par les deux chambres en septembre 2020. Ce projet n'ayant pas suscité de référendum, le Préposé a publié sur son site un bref commentaire des nouvelles dispositions (cf. Accent I). L'entrée en vigueur de la nouvelle LPD et de son ordonnance d'application lui conférera de nouvelles tâches et des compétences de surveillance renforcées, ce qui devrait accroître les besoins en matière de communication et sa présence dans la vie publique. Dans la perspective de cette entrée en vigueur, il a entrepris le remaniement de ses feuillets thématiques, de ses commentaires explicatifs et de ses guides.

Enjeux et conditions de la communication

Le secteur Communication a retrouvé au second semestre 2020 son effectif initial, soit 2,4 équivalents plein temps que se partagent trois personnes. Ce rétablissement permet aussi de mieux représenter le plurilinguisme de la Suisse. Ses ressources étant limitées, le Préposé concentre ses relations publiques sur trois canaux : le (présent) rapport d'activités, le site internet et les relations directes avec les journalistes. Il fait un usage restreint de Twitter mais n'intervient sur aucun autre réseau social, par mesure de protection des données notamment.

Au cours de l'année sous revue, le rapport d'activités a fait l'objet d'un nouvel appel d'offres, ce qui a permis d'améliorer le cadre rédactionnel et conceptuel sans modifier le budget.

Intérêt toujours très vif des médias

Le vif intérêt des médias s'est reflété au cours de l'année sous revue dans les nombreuses communications du Préposé sur des questions d'actualité et dans les nombreux articles et reportages consacrés par la presse papier et numérique à la protection des données en général et au principe de la transparence dans l'administration. Rien que dans son monitoring des médias, qui observe les médias suisses et une sélection de journaux internationaux incontournables, le Préposé a recensé près de 4000 articles. Ce chiffre, deux fois plus élevé que celui de l'année précédente, s'explique moins par la modification du profil de recherche que par l'augmentation très nette de la pertinence. Plus de la moitié de ces articles sont consacrés à la pandémie.

Le Préposé a aussi observé une forte activité sur les réseaux sociaux et les plateformes en ligne (cf. troisième de couverture, chiffre clés). Le PFPDT y est cité 7320 fois, dont 1152 citations directes du Préposé ou d'un porte-parole, et plus de la moitié sur des canaux étrangers. Sur les réseaux sociaux, les «engagements» (nombre d'interactions telles que «likes», partages ou commentaires générés par un post) sont un indicateur clé. Leur nombre (3,36) est très élevé et témoigne d'une interconnexion forte et active dans les communautés.

Le Préposé a traité près de 600 demandes des médias, soit environ un tiers de plus que l'année précédente. La plupart émanaient de journalistes accrédités auprès du centre de presse du Palais fédéral. Les citoyens et les entreprises ont utilisé le courrier électronique ou postal ou la hotline télé-

phonique pour soumettre leurs préoccupations ou leurs questions (près de 4200) aux experts du PFPDT.

Le Préposé a par ailleurs participé à une quarantaine de manifestations organisées par des associations, des établissements de formation, des autorités, des entreprises ou encore des organisations de l'univers numérique.

CORONA

Informations relatives au coronavirus

Le Préposé et ses experts, outre un important travail de consultation relatif à la pandémie, ont publié plusieurs avis sur la conformité de grands enjeux en matière de protection des données, notamment sur les sujets suivants :

- Évaluation des comportements de mobilité sur le territoire suisse : accès de l'OFSP aux données visualisées de Swisscom
- Traçage de proximité : l'application SwissCovid respecte les exigences en matière de protection des données
- Mesures de sécurité pour les conférences audio et vidéo
- Mise en œuvre des plans de protection contre le coronavirus par les entreprises privées : nécessité du consentement à la transmission des données personnelles
- Collecte des coordonnées destinée au traçage des contacts : les exploitants doivent garantir la protection des données, l'utilisation d'applications doit rester volontaire
- Carnet de vaccination électronique : ouverture d'une procédure contre la fondation «mesvaccins»

Dans le cadre de la Journée internationale de la protection des données, le 28 janvier 2021, le Préposé a rappelé avec Privatim, la Conférence des Préposés suisses à la protection des données, la nécessité de protéger la sphère privée pendant la pandémie. Face aux médias, les autorités de protection des données ont insisté sur le droit à la vie privée et à l'autodétermination, dont la restriction ne peut pas perdurer au-delà de la pandémie. Il faut que la population garde la possibilité d'effectuer de vrais choix face aux technologies numériques et d'opter pour des solutions anonymes.

Avis, recommandations et publications

Au cours de l'année sous revue, le Préposé a publié divers avis et déclarations sur des sujets d'actualité. Le coronavirus, bien sûr (cf. encadré), mais aussi les suivants :

- révision totale de la LPD (examen et dispositions) ;
- réglementation insuffisante du traitement des données dans la nouvelle loi sur la police douanière ;
- bouclier de protection des données (Privacy Shield) entre la Suisse et les États-Unis et entre l'UE et les États-Unis, notamment à propos de l'arrêt de la Cour de justice de l'Union européenne concernant les clauses contractuelles types européennes ;
- traitement des données concernant Diem (anciennement Libra) ;
- révision de la loi fédérale sur l'assurance-maladie : transparence des modèles de prix.

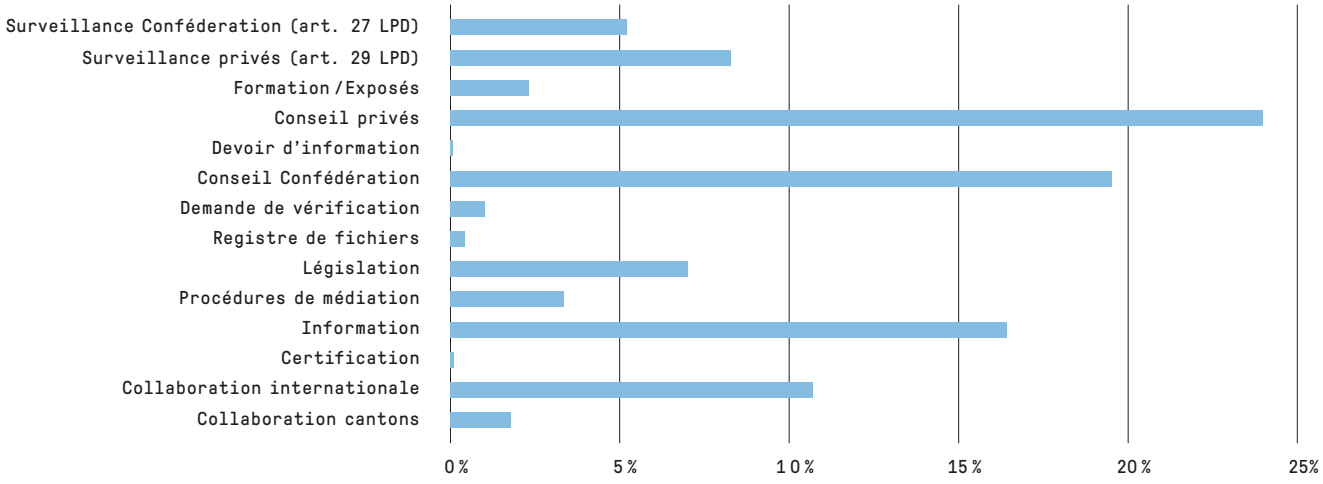
Le PFPDT a en outre publié sur son site 26 recommandations relatives au principe de la transparence.

Le 27e numéro 2019/2020 du rapport d'activités visé à l'art. 30 LPD a été publié le 30 juin 2020, toujours en quatre langues, en version papier et électronique (accessible par un lien sur le site).

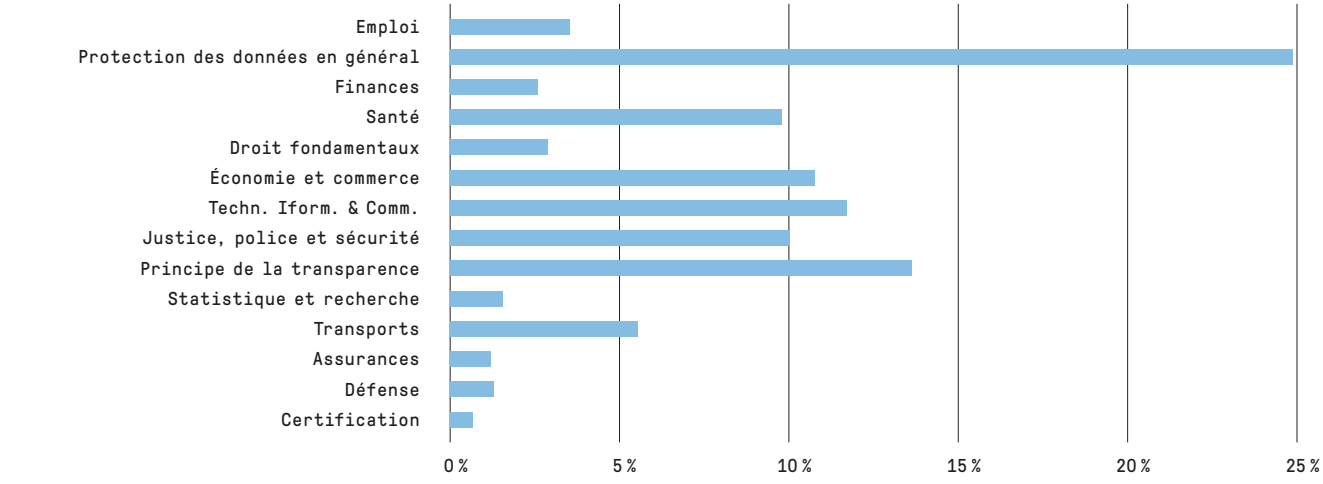
3.3 Statistiques

Statistiques des activités du PFPDT du 1er avril 2020 au 31 mars 2021 (Protection des données)

Charge de travail par tâches

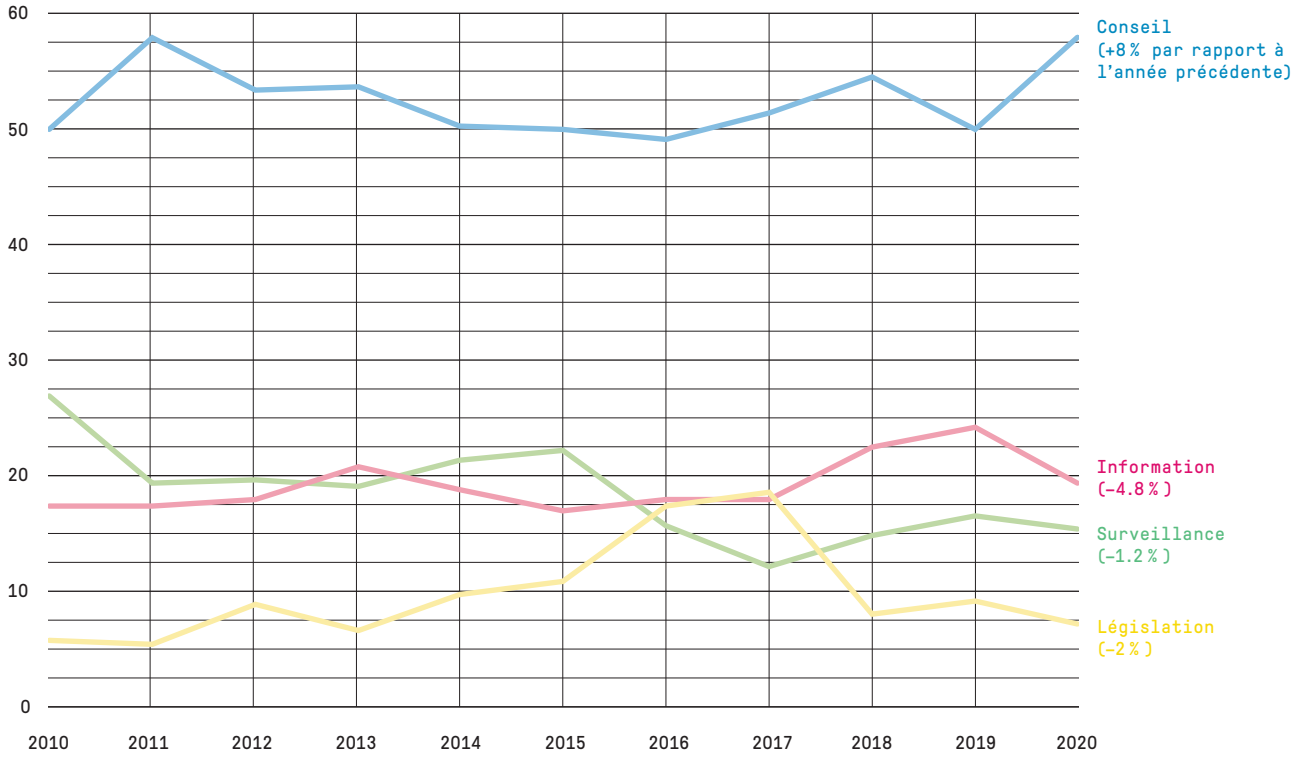


Charge de travail par domaines



Comparaison pluriannuelle

(en pourcentage)



Vue d'ensemble des demandes d'accès du 1er janvier 2020 au 31 décembre 2020

Département	Nombre de demandes d'accès		Accès accordé		Accès refusé		Accès accordé partiellement/différé		Demandes d'accès retirées		Demandes d'accès pendantes		Aucun document officiel disponible	
ChF	31		20		5		4		0		2		0	
DFAE	174		88		14		47		11		4		10	
DFI	312		114		26		100		8		41		23	
DFJP	77		45		11		9		2		3		7	
DDPS	251		184		10		37		5		10		5	
DFF	109		51		13		28		3		6		8	
DEFR	115		49		15		36		3		7		5	
DETEC	105		53		8		32		3		3		6	
MPC	13		6		1		0		0		4		2	
SP	6		0		5		0		0		0		1	
Total 2020 (%)	1193	(100)	610	(51)	108	(9)	293	(24)	35	(3)	80	(7)	67	(6)
Total 2019 (%)	916	(100)	542	(62)	86	(11)	171	(21)	38	(6)	43	(5)	36	(4)
Total 2018 (%)	636	(100)	352	(55)	62	(10)	119	(19)	24	(4)	48	(7)	31	(5)
Total 2017 (%)	581	(99)	317	(55)	107	(18)	106	(18)	26	(4)	21	(4)	–	
Total 2016 (%)	551	(99)	293	(53)	87	(16)	105	(19)	33	(6)	29	(5)	–	
Total 2015 (%)	597	(100)	319	(53)	98	(16)	127	(21)	31	(5)	22	(4)	–	
Total 2014 (%)	575	(100)	297	(52)	122	(21)	124	(22)	15	(3)	17	(3)	–	
Total 2013 (%)	469	(100)	218	(46)	122	(26)	103	(22)	18	(4)	8	(2)	–	
Total 2012 (%)	506	(100)	223	(44)	138	(27)	120	(24)	19	(4)	6	(1)	–	
Total 2011 (%)	466	(100)	203	(44)	126	(27)	128	(27)	0	(0)	9	(2)	–	

Statistique des demandes d'accés selon la loi sur la transparence du 1er janvier 2020 au 31 décembre 2020

	Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Chancellerie fédérale ChF	ChF	**21**	12	5	3	0	1	0
	PFPDT	**10**	8		1		1	
	Total	**31**	**20**	**5**	**4**	**0**	**2**	**0**
Département fédéral des affaires étrangères DFAE	DFAE	**174**	88	14	47	11	4	10
	Total	**174**	**88**	**14**	**47**	**11**	**4**	**10**
Département fédéral de l'interieur DFI	SG DFI	**20**	12	0	5	0	3	0
	BFEG	**4**	3	0	0	1	0	0
	OFC	**3**	1	0	2	0	0	0
	AFS	**3**	1	0	2	0	0	0
	MétéoSuisse	**1**	1	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	OFSP	**181**	51	22	69	3	26	10
	OFS	**7**	4	1	0	0	0	2
	OFAS	**19**	15	0	4	0	0	0
	OSAV	**25**	8	3	9	4	0	1
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**42**	15	0	9	0	10	8
	SUVA	**7**	3	0	0	0	2	2
	Total	**312**	**114**	**26**	**100**	**8**	**41**	**23**
Département fédéral de justice et police DFJP	SG DFJP	**5**	4	0	0	0	0	1
	OFJ	**29**	18	7	2	0	0	2
	FEDPOL	**13**	6	2	2	1	0	2
	METAS	**2**	2	0	0	0	0	0
	SEM	**19**	10	1	5	0	3	0
	Service SCPT	**1**	0	1	0	0	0	0
	ISDC	**5**	3	0	0	0	0	2
	IPI	**2**	2	0	0	0	0	0
	CFMJ	**0**	0	0	0	0	0	0
	CAF	**0**	0	0	0	0	0	0
	ASR	**1**	0	0	0	1	0	0
	CSI	**0**	0	0	0	0	0	0
	CNPT	**0**	0	0	0	0	0	0
	Total	**77**	**45**	**11**	**9**	**2**	**3**	**7**

	Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	**20**	7	0	10	1	0	2
	Défens/armée	**34**	13	0	9	2	9	1
	SRC	**18**	3	8	3	2	0	2
	armasuisse	**12**	9	0	2	0	1	0
	OFSPO	**150**	147	2	1	0	0	0
	OFPP	**17**	5	0	12	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OAC	**0**	0	0	0	0	0	0
	Total	**251**	**184**	**10**	**37**	**5**	**10**	**5**
Département fédéral des finances DFF	SG DFF	**22**	11	1	9	0	1	0
	UPIC	**1**	0	0	1	0	0	0
	AFF	**10**	1	1	7	1	0	0
	OFPER	**1**	1	0	0	0	0	0
	AFC	**10**	7	0	3	0	0	0
	ARD	**37**	15	7	5	1	3	6
	OFCL	**3**	1	1	1	0	0	0
	OFIT	**4**	2	0	0	1	0	1
	CDF	**8**	3	3	1	0	0	1
	SFI	**3**	0	0	1	0	2	0
	PUBLICA	**0**	0	0	0	0	0	0
	DdC	**10**	10	0	0	0	0	0
	Total	**109**	**51**	**13**	**28**	**3**	**6**	**8**
Département fédéral de l'économie, de la formation et de la recherche DEFR	SG DEFR	**9**	6	1	0	1	0	1
	SECO	**35**	16	10	7	1	0	1
	SEFRI	**4**	3	0	0	0	0	1
	OFAG	**14**	3	0	7	0	3	1
	OFAE	**7**	3	0	3	0	0	1
	OFL	**3**	0	0	3	0	0	0
	SPR	**2**	1	0	1	0	0	0
	COMCO	**18**	11	1	3	1	2	0
	CIVI	**0**	0	0	0	0	0	0
	BFC	**2**	2	0	0	0	0	0
	FNS	**2**	1	0	0	0	1	0
	IFFP	**1**	0	0	0	0	1	0
	Conseil ETH	**16**	3	3	10	0	0	0
	Innosuisse	**2**	0	0	2	0	0	0
	Total	**115**	**49**	**15**	**36**	**3**	**7**	**5**

	Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de l'environnement, des transports, de l'energie et de la communication DETEC	SG DETEC	**9**	8	0	1	0	0	0
	OFT	**14**	9	0	3	2	0	0
	OFAC	**9**	3	0	2	0	1	3
	OFEN	**4**	3	0	0	0	0	1
	OFROU	**9**	7	0	2	0	0	0
	OFCOM	**14**	2	2	10	0	0	0
	OFEV	**38**	17	5	13	1	0	2
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	IFSN	**7**	3	1	1	0	2	0
	PostCom	**1**	1	0	0	0	0	0
	AIEP	**0**	0	0	0	0	0	0
	Total	**105**	**53**	**8**	**32**	**3**	**3**	**6**
Ministère public de la Confédération MPC	MPC	**13**	6	1	0	0	4	2
	Total	**13**	**6**	**1**	**0**	**0**	**4**	**2**
Services du Parlament SP	SP	**6**	0	5	0	0	0	1
	Total	**6**	**0**	**5**	**0**	**0**	**0**	**1**
	Somme totale	**1193**	**610**	**108**	**293**	**35**	**80**	**67**

Demandes d'accès 2020 avec référence Corona

	Section concernée	Demandes avec référence Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Chancellerie fédérale ChF	ChF	**6** (100%)	3 (50%)	3 (50%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PFPDT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**6** (100%)	**3** (50%)	**3** (50%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Département fédéral des affaires étrangères DFAE	DFAE	**13** (100%)	12 (92%)	1 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**13** (100%)	**12** (92%)	**1** (8%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Département fédéral de l'interieur DFI	SG DFI	**17** (10%)	11 (6%)	0 (0%)	3 (2%)	0 (0%)	3 (2%)	0 (0%)
	BFEG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	MétéoSuisse	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BN	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFSP	**134** (77%)	44 (25%)	16 (9%)	53 (31%)	1 (1%)	11 (6%)	9 (5%)
	OFS	**1** (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)
	OFAS	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OSAV	**4** (2%)	3 (2%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	MNS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SWISS MEDIC	**16** (9%)	4 (2%)	0 (0%)	0 (0%)	0 (0%)	9 (5%)	3 (2%)
	SUVA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**174** (100%)	**64** (37%)	**17** (10%)	**56** (32%)	**1** (1%)	**23** (13%)	**13** (7%)
Département fédéral des finances DFF	SG DFF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	UPIC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFF	**9** (36%)	1 (4%)	1 (4%)	6 (24%)	1 (4%)	0 (0%)	0 (0%)
	OFPER	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AFC	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ARD	**11** (44%)	1 (4%)	5 (20%)	3 (12%)	0 (0%)	0 (0%)	2 (8%)
	OFCL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFIT	**3** (12%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)	0 (0%)	0 (0%)
	CDF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SFI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PUBLICA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	DdC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**6** (11%)	**6** (11%)	**9** (16%)	**2** (4%)	**0** (0%)	**2** (4%)

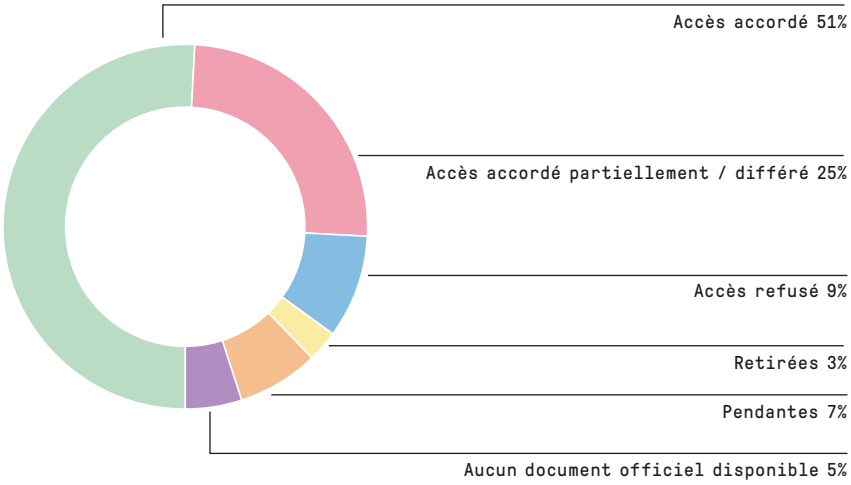
	Section concernée	Demandes avec référence Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de justice et police DFJP	SG DFJP	**1** (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (14%)
	OFJ	**6** (86%)	5 (71%)	1 (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FEDPOL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METAS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SEM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Service SCPT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ISDC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IPI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CFMJ	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CAF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ASR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CSI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CNPT	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**7** (100%)	**5** (71%)	**1** (14%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (14%)
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFT	**2** (50%)	1 (25%)	0 (0%)	0 (0%)	1 (25%)	0 (0%)	0 (0%)
	OFAC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFEN	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFROU	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFCOM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFEV	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ARE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ComCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IFSN	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PostCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	AIEP	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**4** (100%)	**3** (75%)	**0** (0%)	**0** (0%)	**1** (25%)	**0** (0%)	**0** (0%)
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	**8** (16%)	1 (2%)	0 (0%)	5 (10%)	0 (0%)	0 (0%)	2 (4%)
	Défens/ armée	**23** (46%)	10 (20%)	0 (0%)	3 (6%)	1 (2%)	8 (16%)	1 (2%)
	SRC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	armasuisse	**1** (2%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFSPO	**3** (6%)	3 (6%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFPP	**15** (30%)	3 (6%)	0 (0%)	12 (24%)	0 (0%)	0 (0%)	0 (0%)
	swisstopo	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OAC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**50** (100%)	**18** (36%)	**0** (0%)	**20** (40%)	**1** (2%)	**8** (16%)	**3** (6%)

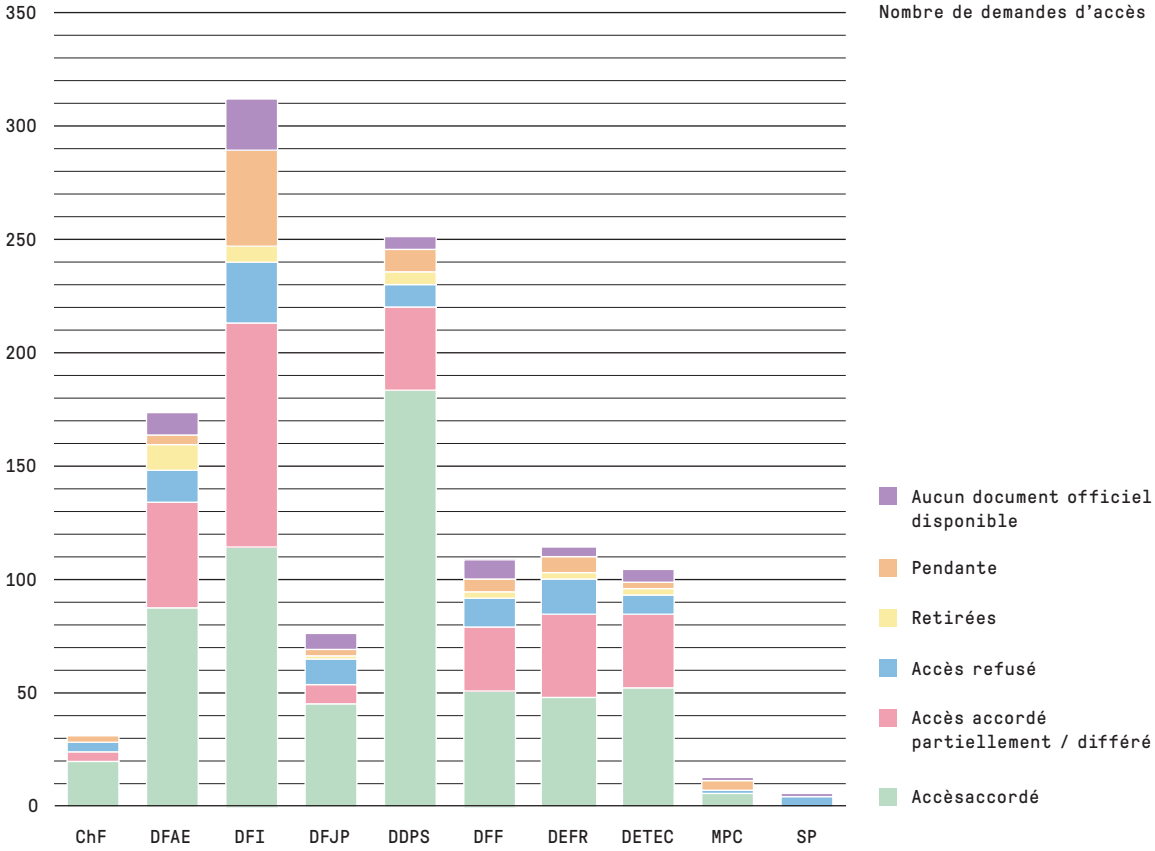
	Section concernée	Demandes avec référence Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de l'économie, de la formation et de la recherche DEFR	SG DEFR	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SECO	**14** (56%)	5 (20%)	7 (28%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)
	SEFRI	**1** (4%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFAG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFAE	**5** (20%)	2 (8%)	0 (0%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)
	OFL	**3** (12%)	0 (0%)	0 (0%)	3 (12%)	0 (0%)	0 (0%)	0 (0%)
	SPR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	COMCO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CIVI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	BFC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FNS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IFFP	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Conseil ETH	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Innosuisse	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**10** (40%)	**7** (28%)	**7** (28%)	**0** (0%)	**0** (0%)	**1** (4%)
Ministère public de la Confédération MPC	MPC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Services du Parlament SP	SP	**4** (100%)	0 (0%)	3 (75%)	0 (0%)	0 (0%)	0 (0%)	1 (25%)
	Total	**4** (100%)	**0** (0%)	**3** (75%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (25%)

Nombre de demandes en médiation

Catégories de requérants	2020
Médias	**31**
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	**42**
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	**5**
Avocats	**7**
Entreprises	**7**
Universités	**1**
Total	**93**

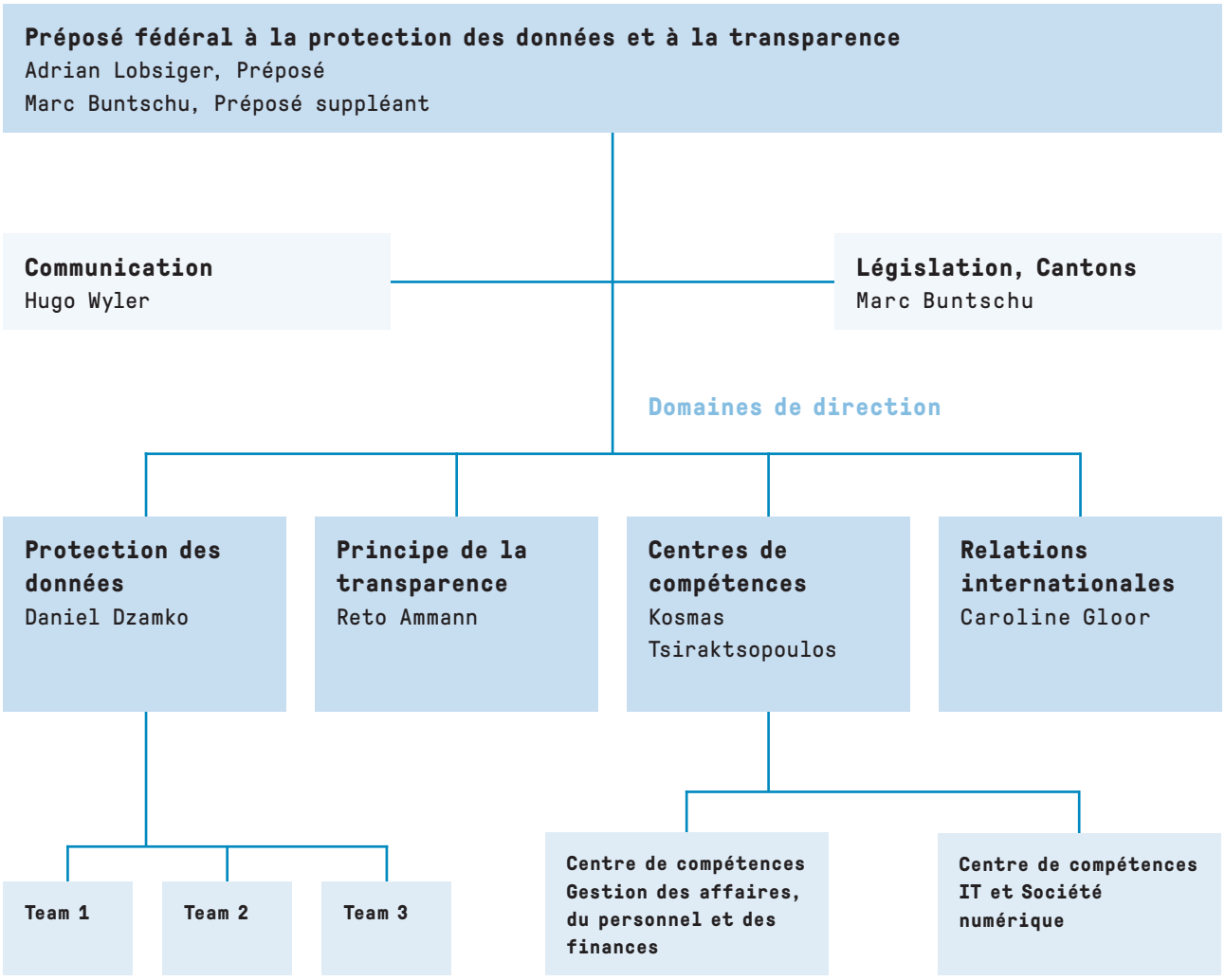
Traitment des demandes d'accès
du 1er janvier 2020 au 31 décembre 2020





3.4 Organisation du PFPDT (État 31 mars 2021)

Organigramme



Personnel du PFPDT

Nombre d'employés	38		
FTE	31.8		
par sexe	Femmes	20	53 %
	Hommes	18	47 %
par niveau d'emploi	1–89 %	25	63 %
	90–100 %	13	37 %
par langue	Allemend	30	79 %
	Français	7	18 %
	Italien	1	3 %
par âge	20–49 ans	24	63 %
	50–65 ans	14	37 %
Postes dirigeants	Femmes	3	33 %
	Hommes	6	67 %

Liste des abréviations

AMVP Assemblée mondiale pour la protection de la vie privée

BCR règles d'entreprise contraignantes (Binding Corporate Rules)

CCT clauses contractuelles types

CEPD Comité européen de la protection des données

CEPD Contrôleur européen de la protection des données

CJUE Cour de justice de l'Union européenne

Convention 108+ convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Datareg registre des banques de données

DEP dossier électronique du patient

IA intelligence artificielle

LDEP loi fédérale sur le dossier électronique du patient

LEp loi fédérale sur la lutte contre les maladies transmissibles de l'homme (loi sur les épidémies)

LPD révisée loi sur la protection des données révisée

LPD loi sur la protection des données

LPDS loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal

LSIE loi fédérale sur les services d'identification électronique (loi sur l'e-ID)

LTrans loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence)

LTV loi sur le transport de voyageurs

NaDB Programme de gestion nationale des données

NAVS13 numéro AVS à 13 chiffres

NCSC Centre national pour la cybersecurité

PNR données des passagers des compagnies aériennes (Passenger Name Record)

Privatim Conférence des Préposé-e-s suisses à la protection des données (autorités cantonales)

RGPD règlement général sur la protection des données

SRC Service de renseignement de la Confédération

TIC technologies de l'information et de la communication

Table des illustrations

Graphiques

Tableaux

Impressum

Ce rapport est disponible en quatre langues et peut être consulté sur Internet (www.leprepose.ch).
Distribution: OFCL, Vente des publications fédérales, CH-3003 Berne
www.bundespublikationen.admin.ch
Art.-Nr. 410.028.F

Mise en page: Ast & Fischer AG, Wabern
Photographie: Nicolas Stadler
Caractères: Pressura, Documenta
Impression: Ast & Fischer AG, Wabern
Papier: PlanoArt®, holzfrei hochweiss

Chiffres clés

Dépenses de protection des données

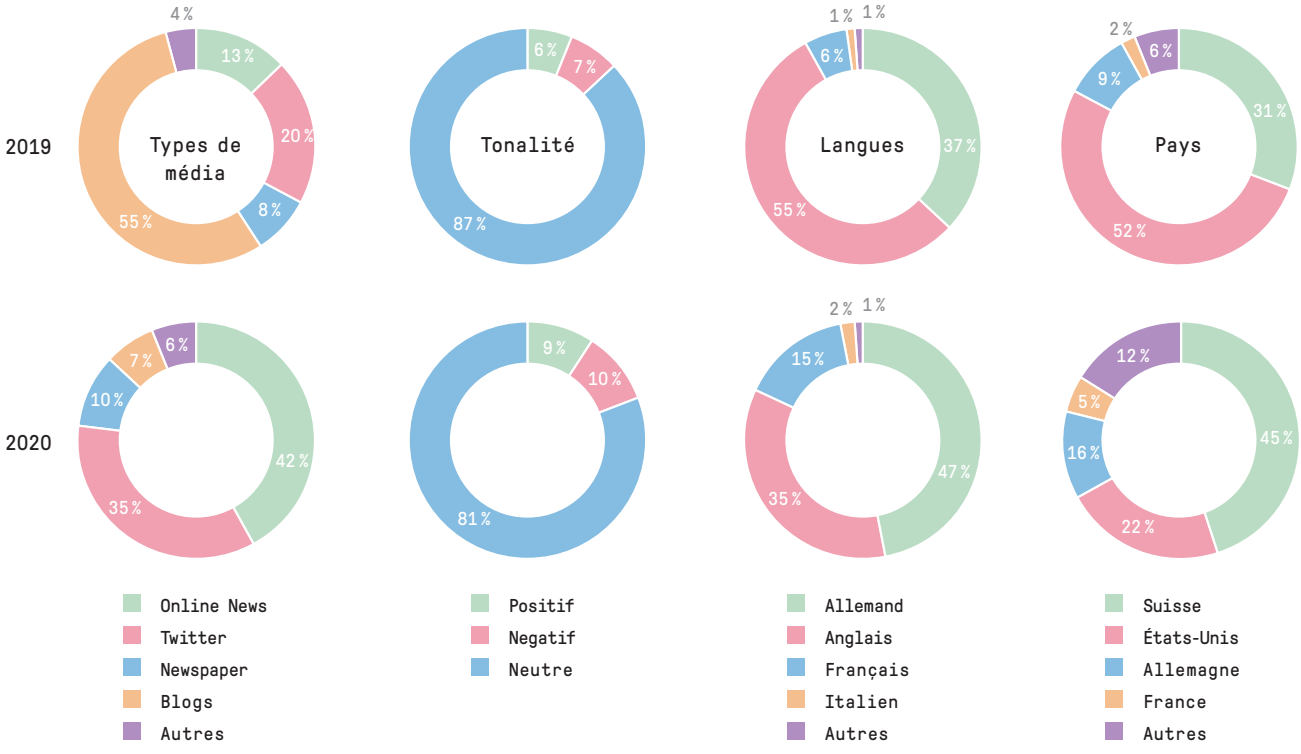
57,8 %	15,0 %	19,4 %	7,3 %
Conseils	Surveillance	Information	Législation

Demandes d'accès Principe de la transparence (LTrans)

51 %	25 %	9 %	3 %	7 %	5 %
accordé	accordé partiellement/ differé	refusé	retirées	pendantes	aucun document officiel disponible

Résonance médiale du Préposé sur le web social

* Nombre de toutes les mentions du PFPDT (mentions dans Blogs, Twitter, Onlinenews, etc.)
** Nombre de toutes les interactions des contributions examinées (Likes, Retweets, etc.)



Préoccupations relatives à la protection des données

Transparence de l'information

Les entreprises et les autorités fédérales fournissent des informations transparentes sur le traitement de leurs données : c'est compréhensible et complet.

Possibilité de choisir

Les personnes concernées donnent leur consentement et jouissent d'une réelle liberté de choix.

Analyse des risques

Les risques éventuels pour la protection des données sont déjà identifiés dans le projet et leurs effets sont minimisés par des mesures.

Exactitude des données

Le traitement s'effectue avec des données correctes.

Proportionnalité

Pas de collecte systematique de données, seulement dans la mesure où cela est nécessaire pour atteindre l'objectif. Le traitement des données est limité dans le temps et dans l'espace.

Finalité

Les données ne seront traitées qu'aux fins indiquées au moment de la collecte, selon les circonstances ou dans les cas prévus par la loi.

Sécurité des données

Les responsables du traitement des données veillent techniquement et organisationnellement à ce que les données personnelles soient protégées de manière adéquate.

Documentation

Tout traitement de données est documenté et classé par le responsable du traitement des données.

Responsabilité individuelle

Les organismes privés et fédéraux sont responsables du respect de leur obligation de se conformer à la législation sur la protection des données.

Préposé fédéral à la protection des données et à la transparence
Feldeggweg 1
CH-3003 Berne

E-Mail: info@edoeb.admin.ch
Website: www.leprepose.ch
@derBeauftragte
Téléphone: +41 (0)58 462 43 95 (Lu – Ve, 10 – 12 heures)
Téléfax: +41 (0)58 465 99 96