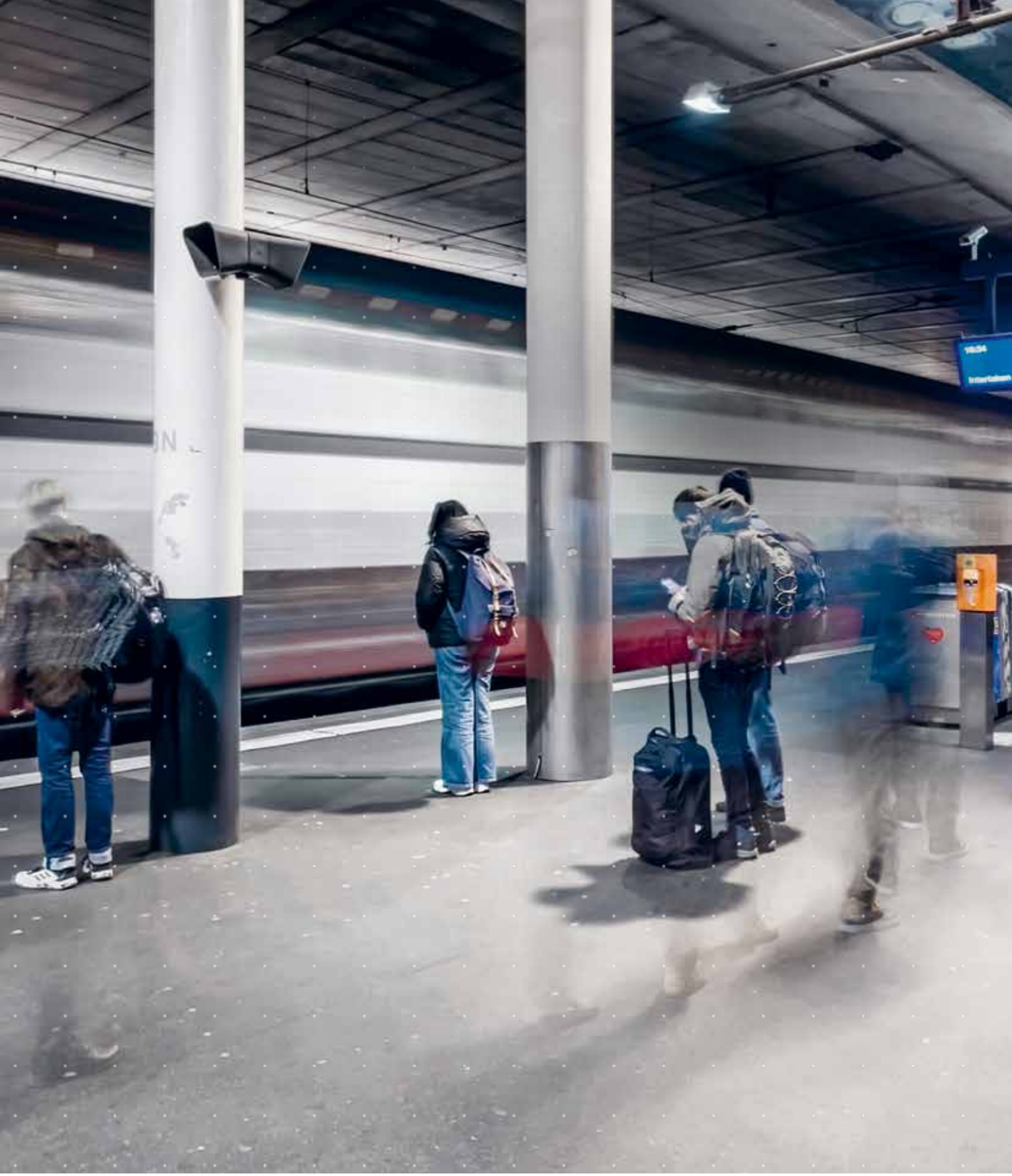


29e Rapport d'activités 2021/22

Préposé fédéral à la protection des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2021/2022
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 2021 au 31 mars 2022.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Avant-propos

Alors que la pandémie qui entrave notre santé et nos loisirs semble toucher à sa fin, la Suisse numérique remporte un succès d'estime sur le plan de la protection des données avec l'application SwissCovid et le certificat COVID (y compris sa version « light »). La conception sobre en données et décentralisée de ces outils a permis d'éviter de transmettre à l'administration fédérale des données concernant les citoyens, et de limiter la communication de données de santé à des acteurs privés à un niveau compatible avec la protection des données.

La Suisse numérique doit par ailleurs reconnaitre des failles, tant au niveau technique qu'organisationnel, dans l'exploitation de certaines applications de traçage des contacts ainsi que des registres de vaccination, de dons d'organes et d'implants mammaires. Depuis que le journalisme d'enquête a révélé au grand public avec quelle facilité des personnes non autorisées pouvaient accéder à des données sensibles, tous les exploitants de plateformes ont vraisemblablement compris qu'ils devaient assumer leurs responsabilités. Il est également important que l'instauration attendue d'une identité électronique reconnue par l'État aboutisse lors de la seconde tentative.

La transformation numérique de nos univers de travail et de loisirs s'est accélérée dans le sillage de la pandémie. L'annonce du « métavers » a sonné le glas des plateformes sociales actuelles, fondés sur des applications. La prochaine génération de cyber-réseaux invite les humains à enfiler des lunettes de réalité virtuelle ultralégères et à se rencontrer dans des espaces virtuels dans lesquels des signaux numériques se superposent à l'environnement physique, créant ainsi un monde « amélioré ». Comment ces lunettes capteront-elles notre environnement privé ? Comment les intelligences artificielles enregistreront et interpréteront-elles dans le nuage nos mimiques, nos voix et notre comportement ? Les gens finiront-ils par percevoir le monde réel comme gris, solitaire et menaçant ?

Ces questions de la surveillance fédérale de la protection des données expriment la volonté de la population à participer à la définition de la réalité numérique de demain.

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

Berne, le 31 mars 2022

Protection des données

Principe de la transparence

Le PFPDT

Défis actuels

I Numérisation

Le quotidien de la plupart des personnes en Suisse est façonné par l'utilisation de technologies de l'information et de la communication (TIC). Le numérique a investi notre société, et ce mouvement n'est pas près de s'arrêter : il a plutôt vocation à perdurer sous la forme d'une succession de réalités numériques évolutives.

Le smartphone est-il proche du déclin?

L'exemple du smartphone, qui fut le moteur de la diffusion du numérique dans la société ces quinze dernières années, illustre parfaitement ce processus. Pendant la période sous revue, la génération de données par le biais de cet appareil s'est encore intensifiée puisque l'accès aux manifestations publiques et aux restaurants a dépendu, des mois durant, de la présentation d'un certificat COVID, généralisant ainsi l'habitude de porter son smartphone allumé sur soi lors de déplacements. D'autre part, la large couverture médiatique dont a fait l'objet l'émergence du « métavers » semble indiquer que même le smartphone est appelé à décliner : selon les promoteurs de cette réalité parallèle, l'homme va peu à peu se détacher des plateformes sociales basées sur des applications et abandonner écrans, claviers et souris pour s'immerger dans des espaces virtuels en chaussant de simples lunettes.

« Métavers » versus monde réel

Le géant de la communication Facebook a récemment adopté le nom de « Meta » dans le double but de gagner des investisseurs et des utilisateurs pour sa propre partie du futur métavers mondial, et d'y établir des droits commerciaux.

Dans la prochaine génération de cyber-réseaux, les humains se rencontreront dans des espaces virtuels, dans lesquels des signaux numériques se superposeront à leur environnement physique, créant ainsi un monde hybride et meilleur appelé « réalité augmentée ». Ils seront censés percevoir ce nouvel environnement comme réel alors qu'ils n'y croiseront que des avatars purement virtuels, et non des êtres de chair et de sang. Ces rencontres pourront avoir lieu dans des appartements privés ou des locaux publics. À cette fin, des capteurs sonderont et mesureront les espaces et diffuseront les données collectées sur Internet en temps réel. C'est une évidence : le concept du métavers implique une ingérence dans la vie privée de milliards d'individus.

Tout un chacun pourra s'immerger en quelques secondes dans le métavers en enfilant une « simple » paire de lunettes. Le comportement des adeptes de jeux virtuels donne une idée de ce que cela signifie à terme pour le monde réel non digital : si l'homme finit par le percevoir comme terne et solitaire, il y passera de moins en moins de temps. La méta-société jugera-t-elle un jour le monde réel comme dangereux car dépourvu de certains signaux d'alerte ?

Pour mettre en scène la réalité augmentée, les lunettes VR et leurs capteurs enregistreront les regards, les mimiques et les postures, mais aussi les lectures et les aliments consommés par leur hôte humain. Toutes ces données sensibles aboutiront un jour dans le cloud des exploitants de réseaux sociaux, et ce dans des proportions incommensurablement supérieures à ce qui se passe dans la réalité numérique d'aujourd'hui.

Plus les individus transposeront leur vie sociale dans des univers numériques, plus ils s'exposeront à des

« Le concept du ‹ métavers › implique une ingérence dans la vie privée de milliards d'individus. »

atteintes à la personnalité. Par exemple, lorsqu'ils utiliseront un avatar photoréaliste, dont le perfectionnement n'est plus qu'une question de temps. Dans ce contexte, le PFPDT œuvrera en amont, en collaboration avec d'autres autorités de surveillance, pour que les fournisseurs d'univers numériques fassent preuve de transparence quant aux risques qui y sont liés et prennent des mesures afin de protéger la sphère privée et le droit à l'autodétermination des utilisatrices et utilisateurs.

Stratégie Suisse numérique

Pour que la population suisse puisse profiter des avantages de la numérisation, le Conseil fédéral a élaboré une stratégie Suisse numérique qu'il met à jour régulièrement et qui engage les autorités de tous les échelons de l'État fédéral, la société civile et les milieux économique, scientifique et politique à faire avancer conjointement la transformation numérique.

Selon cette stratégie, la transformation numérique des structures existantes exige un changement de mentalité qui remet en question les formes traditionnelles de cohabitation et de gestion. L'heure est à l'acquisition de compétences numériques, à la mise en réseau et au partage de données entre tous les acteurs. L'accumulation de connaissances qui en résulte doit donner naissance à une Suisse dans laquelle la population participe également à la vie sociale, politique et économique dans l'espace numérique.

Le service public, partenaire discret de la population

Aux antipodes de cette vision stratégique figure, selon nombre de promoteurs de la transformation numérique, la conservation de données en « silos », toutefois mal vue et qu'ils associent à un mode de pensée dépassé et au stéréotype d'une administration fédérale passéiste. Ils ont malheureusement tendance à oublier que les barrières à l'information, prétendument obsolètes, peuvent constituer des piliers systémiques de l'état de droit moderne. Celui-ci a remplacé les régimes aristocratiques où la souveraineté était concentrée dans les mains d'un prince. Ce dernier pouvait à tout moment se saisir d'une affaire, prendre connaissance de l'intégralité des éléments et imposer sa loi aux sujets concernés. Seule l'instauration d'une justice indépendante et la division de l'administration en services spécialisés, conformes à l'état de droit, ont permis la transformation de l'État en un service public et celle des sujets en citoyens.

L'État fondé sur la séparation des pouvoirs se présente aujourd'hui comme un conglomérat de services qui aident les citoyens à exercer leurs droits et leurs devoirs découlant de lois spéciales. La spécialisation de l'administration et la segmentation des informations détenues par les autorités se sont accompagnées d'une transformation du pouvoir de l'État sur la société civile, qui fait aujourd'hui valoir ses droits avec assurance en sollicitant (au besoin devant les tribunaux) l'aide professionnelle et discrète des services spécialisés en échange des taxes acquittées.

État de droit : mise en réseau des données factuelles plutôt que des données des citoyens

Compte tenu de ce contexte historique, la protection des données doit soutenir de manière différenciée l'exigence stratégique d'impliquer davantage l'État et l'administration dans la mise en réseau, le partage et l'utilisation des données. Elle vise à ce que cette dynamisation des informations ne se concentre pas sur les données personnelles mais sur des données factuelles,

« Si les gens perçoivent le monde réel comme terne et solitaire, la durée de leur engagement dans le ‹métavers› augmente. »

en respectant les barrières à l'information prévues par l'état de droit, qui permettent à la société civile de faire valoir ses droits face aux autorités.

La protection des données vise à préserver les droits fondamentaux, qui sont refusés aux personnes vivant dans des États autoritaires, car dans ces États, les personnes se voient encore aujourd'hui restreindre l'accès à des services, à des subventions, à des formations, voire à des prestations sociales ou à des soins médicaux sur la base d'informations dont la quantité et la source leur sont inconnus. Les réseaux numériques et des technologies de surveillance bon marché ont permis à ces États d'intensifier le contrôle sur leur population dans une mesure qui, espérons-le, continuera longtemps de rebuter l'Occident. À titre d'exemple, dans un projet de règlement sur l'intelligence artificielle, la Commission européenne s'est vue dans l'obligation d'interdire aux États membres de l'Union européenne, la surveillance permanente de la population en vue d'une notation sociale, de même que l'utilisation généralisée en temps réel des technologies de reconnaissance faciale dans l'espace public.

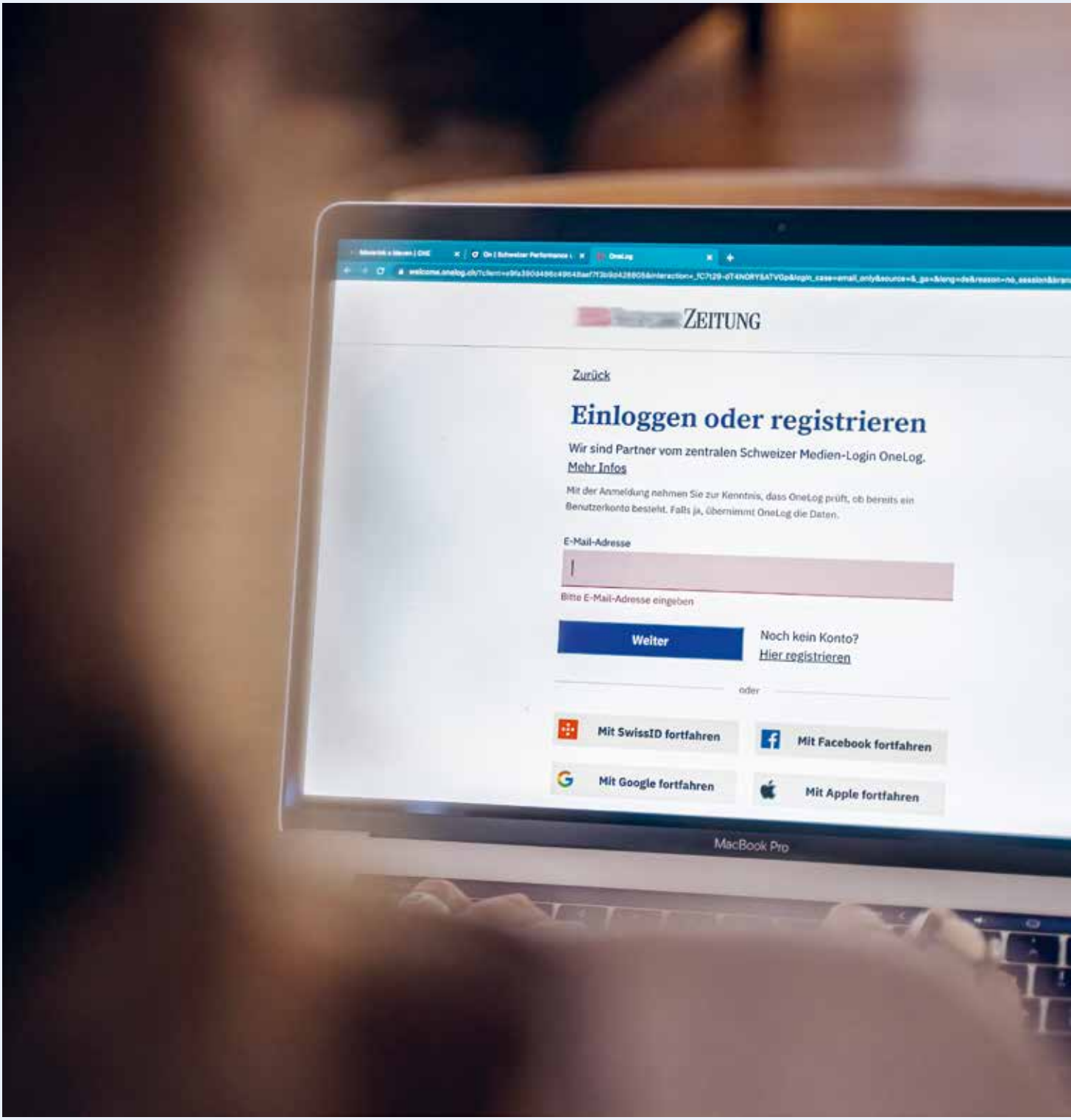
Communiquer sous le couvert de l'anonymat est un droit et non un « abus de liberté »

Du point de vue de la protection des données, il est également indispensable que les démocraties occidentales préservent le droit des acteurs privés de traiter leurs propres données et celles de leurs clients de manière autonome, en étant libres de les cacher à des tiers, y compris à l'État. La criminalité est immanente à la société et ne peut donc en aucun cas servir d'excuse pour reprocher aux citoyens d'« abuser de leur liberté » lorsqu'ils utilisent des systèmes cryptés pour communiquer. Lorsqu'une personne se rend à pied dans un restaurant puis, en bus, dans un lieu où elle commet intentionnellement une infraction, on ne peut pas lui reprocher de déplacement abusif dans l'espace public, ni de repas abusif, ni d'usage abusif des transports publics. Il en va de même lorsqu'un délinquant utilise un canal de communication crypté avant ou après avoir commis un délit. Dans un monde libre, chaque individu devrait avoir le droit de se déplacer sous couvert de l'anonymat, et dans l'univers analogique et dans l'univers numérique, sans avoir à craindre que ses propres déclarations puissent être retenues contre lui. Et dans ce monde libre, il n'y a pas non plus de place pour des géants de la tech qui utilisent l'intelligence artificielle pour rechercher des contenus interdits dans les téléphones mobiles qu'ils ont vendus, afin de dénoncer leurs propriétaires à la police.

Le droit de communiquer de façon anonyme n'exclut pas, bien entendu, les interventions policières au cas par cas, autorisées par le juge, contre des personnes soupçonnées d'infraction et leur entourage.

Mais si en Suisse, des acteurs privés sont empêchés de protéger leurs informations privées et celles de leurs clients sans justification juridique suffisamment claire, le PFPDT est prêt à intervenir dans le cadre de ses compétences légales. À ce propos, il appelle à une mise en œuvre nuancée et réfléchie des stratégies numériques afin qu'elles renforcent la vie privée et le droit à l'autodétermination de la population suisse, plutôt que de les miner.

« La protection des données vise à préserver les droits fondamentaux, qui sont refusés aux personnes vivant dans des États autoritaires. »


ZEITUNG
Zurück
Einloggen oder registrieren
Wir sind Partner vom zentralen Schweizer Medien-Login OneLog.
Mehr Infos
Mit der Anmeldung nehmen Sie zur Kenntnis, dass OneLog prüft, ob bereits ein Benutzerkonto besteht. Falls ja, übernimmt OneLog die Daten.
E-Mail-Adresse
Bitte E-Mail-Adresse eingeben
Weiter
Noch kein Konto?
Hier registrieren
oder
Mit SwissID fortfahren
Mit Facebook fortfahren
Mit Google fortfahren
Mit Apple fortfahren
MacBook Pro

II Activités de conseil, de contrôle 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, le PFPDT a poursuivi l'accompagnement de nombreux projets de big data des autorités fédérales et d'entreprises privées, 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.

La surveillance ne satisfait que partiellement les attentes justifiées du public

Après une nette baisse des charges affectées aux tâches de surveillance au cours de la période 2015–2016, le PFPDT est parvenu à les augmenter légèrement ces deux dernières années, en les stabilisant à un niveau faible en raison de l'insuffisance persistante des moyens. Pendant la période sous revue, il n'a pas été à même de répondre dans la mesure souhaitée aux attentes légitimes du public (cf. ch. 3.1). Tout en approfondissant la bonne collaboration avec le Centre national pour la cybersécurité, le PFPDT ne dispose pas de moyens suffisants pour effectuer des contrôles aléatoires et systématiques de la sécurité technique qu'exigent pourtant les bases de données sensibles, comme par exemple dans le domaine de la santé. Rappelons à ce propos le cas de la fondation « mesvaccins.ch », qui se trouve en liquidation, auquel s'est ajouté, pendant la période sous revue, le scandale des accès incontrôlés aux registres des dons d'organes et des implants mammaires (cf. ch. 1.4).

La hausse des demandes en médiation entraîne des retards de traitement

La pandémie a contraint le Préposé à la transparence à suspendre temporairement ses activités de médiation orales, ce qui a entraîné une diminution des solutions à l'amiables. Par conséquent, le PFPDT a formulé davantage de recommandations par écrit, ce qui, joint à une hausse des demandes en médiation et à des ressources humaines restreintes, a entraîné dans bien des cas un dépassement des délais légaux de traitement. La hausse des demandes ne semblant pas près de s'arrêter, il faut s'attendre à une aggravation de ces retards, faute de ressources supplémentaires.

« Les stratégies numériques doivent être mises en œuvre de manière différenciée et réfléchie. Elles doivent renforcer la vie privée et autodéterminée, et non la miner. »

III Coopération nationale et internationale

Coopération nationale

L'informatique en nuage est l'un des sujets qui préoccupent le PFPDT et ses homologues cantonaux dans le cadre de la transformation numérique. Le bureau de la Conférence des préposés suisses à la protection des données (privatim) a entièrement remanié son aide-mémoire sur les risques et les mesures spécifiques à la technologie du cloud et en a adopté la nouvelle version en février 2022. Le Préposé avait pris position sur le projet avec voix consultative. Dans ce cadre, les contacts bien établis ont permis une bonne collaboration. Le PFPDT s'est penché sur le thème du cloud, notamment en lien avec l'informatique en nuage au sein de l'administration fédérale (cf. ch. 1.1).

Conseil de l'Europe

Le PFPDT reste très actif au sein du Conseil de l'Europe. Il a participé à toutes les 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). En 2021, le Comité des ministres du Conseil de l'Europe a adopté deux documents sur lesquels le comité consultatif avait travaillé : la déclaration relative à la protection du droit au respect de la vie privée des enfants dans l'environnement numérique et la nouvelle recommandation sur la protection des données dans le contexte du profilage.

Coopération internationale

La communication de données personnelles aux pays ne présentant pas un niveau de protection de données adéquat soulève des questions semblables dans différents États. Le PFPDT suit attentivement l'évolution de ce sujet, surtout dans les pays membres de l'Union européenne (UE) ou de l'Espace économique européen. Il a notamment analysé les nouvelles clauses contractuelles types publiées par la Commission européenne afin de voir dans quelle mesure il peut les reconnaître en Suisse (cf. ch. 1.8).

Évaluation du niveau de protection des données

Le rapport de la Commission européenne sur l'adéquation du niveau de protection des données en Suisse a encore pris du retard. En attendant sa publication, la décision d'adéquation de la Commission prise en vertu de la directive 95/46/CE sur la protection des données à laquelle a succédé le Règlement général de l'UE sur la protection des données (RGPD), reste en vigueur. La Commission publiera sans doute simultanément et, il faut l'espérer, avant la fin 2022, les rapports d'adéquation de tous les États considérés comme adéquats avant le RGPD.

Protection des données

1.1 Numérisation et droits fondamentaux

TRANSFORMATION NUMÉRIQUE

Le PFPDT a veillé au respect de la protection des données dans de nombreux projets de transformation numérique de la Confédération

Le grand nombre des projets de transformation numérique de l'administration fédérale est un défi pour l'autorité de taille modeste qu'est le PFPDT. Dans le cadre de son activité de surveillance, le Préposé veille à la prise en compte précoce et systématique des aspects relevant de la loi sur la protection des données. Il entretient à cet effet des contacts avec le nouveau secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale, avec l'Office fédéral de l'informatique et de la télécommunication (OFIT) et avec les offices fédéraux chefs de projet, afin qu'ils l'informent suffisamment tôt des projets de transformation numérique et qu'ils le tiennent au courant des travaux en cours ou prévus.

La stratégie d'informatique en nuage de l'administration fédérale, qui vise à permettre l'utilisation de services en nuage, est un élément important de la transformation numérique. Le PFPDT a donné son avis sur des interventions relatives à l'attribution de services de nuages publics à des entreprises américaines ou chinoises, et à l'utilisation des services cloud de Microsoft. Il a en outre formulé des exigences découlant du droit de la protection des données concernant l'utilisation des services en nuage par les autorités (cf. Accent II).

Après le rejet de la loi fédérale sur les services d'identification électronique lors de la votation du 7 mars 2021, le Département fédéral de justice et police s'est rapidement attelé à l'élaboration d'une nouvelle solution. Le PFPDT profite de cette occasion pour apporter son expertise ; il a par ailleurs exposé publiquement ses priorités à cet égard (cf. ch. 1.1).

Le projet de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA) vise à promouvoir le traitement électronique des processus de la Confédération (principe de la priorité au numérique). Le PFPDT a émis des critiques sur différents aspects dans le cadre de la consultation des offices. Ses remarques ont donné lieu à plusieurs modifications concernant notamment les projets pilotes, la garantie d'un niveau de protection des données approprié, les responsabilités et l'accès aux données de l'Office fédéral de la statistique à des fins statistiques (cf. ch. 1.1).

Le but est de faire appliquer les principes de la collecte unique des données et de leur utilisation multiple. Outre ses atouts, le projet comporte aussi des risques pour la population, comme le PFPDT l'a fait efficacement remarquer à propos du projet pilote de relevé des données fiscales (cf. ch. 1.1).

Projets spécifiques à un domaine

Parmi les grands projets spécifiques à un domaine qui présentent des risques importants du point de vue du droit de la protection des données figurent la révision totale de la loi sur les douanes et la révision partielle de la loi sur le renseignement. Toutes deux visent notamment à moderniser les systèmes informatiques. En accompagnant de près les deux projets, le PFPDT a pu y apporter des améliorations considérables du point de vue du droit de la protection des données (cf. ch. 1.2).

Le principal projet de transformation numérique dans le domaine de la santé est sans doute celui du dossier électronique du patient, qui a pris énormément de retard. Le PFPDT accompagne les travaux de mise en œuvre et discute régulièrement des difficultés liées à la protection des données avec les autorités et les acteurs privés concernés. Il s'est exprimé sur le développement des bases légales et des systèmes lors de différentes consultations.

Les risques de la transformation numérique pour la protection des données ne pèsent pas uniquement sur la population mais aussi sur les collaborateurs de l'administration fédérale. Le PFPDT s'est exprimé sur le cadre juridique, du point de vue de la protection des données, et sur le suivi d'un projet pilote de création d'un réseau de savoir-faire (cf. ch. 1.1).

TRANSFORMATION NUMÉRIQUE

Loi fédérale sur l'utilisation des moyens électroniques

Le Département fédéral des finances a soumis pour avis au PFPDT le projet de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA), qui fixe de nombreux objectifs dans le domaine de la transformation numérique de l'administration fédérale. Le Préposé a donné son avis et demandé un certain nombre d'améliorations et de précisions, dont l'administration a approuvé le principe.

La LMETA est un projet transversal qui vise à l'emploi efficace et moderne des données par-delà les frontières des unités administratives dans le cadre de la transformation numérique de l'administration fédérale et du développement de ses services numériques. Elle crée les bases nécessaires à la publication de données de l'administration en vue de leur libre utilisation (données publiques en libre accès) et à la mise à disposition et à l'utilisation de moyens informatiques des autorités fédérales. Elle consacre aussi le principe de l'échange électronique automatisé des données au moyen d'interfaces et règle l'exploitation d'une plateforme d'interopérabilité.

Le PFPDT reconnaît la nécessité de la transformation numérique de l'administration fédérale et l'utilité de l'interopérabilité numérique des données. Il rappelle cependant régulièrement qu'il faut identifier à temps et mettre en évidence les risques que présentent ces objectifs pour les droits des personnes concernées. Aussi a-t-il souligné à plusieurs reprises dans sa prise de position sur la LMETA la nécessité de procéder à une analyse d'impact des risques. Il estime par ailleurs que le projet de loi ne fait pas suffisamment la distinction entre données techniques et données personnelles, ce qui pose des problèmes de délimitation par rapport à la loi sur la protection des données (LPD). Le Préposé a par conséquent demandé des précisions sur différents points.

Pas d'extension des accès aux données

Dans l'esprit du principe de la collecte unique des données en vue d'une utilisation multiple, le projet de LMETA prévoit de créer dans la loi sur la statistique fédérale une base légale qui permettra à l'Office fédéral de la statistique (OFS) d'accéder en ligne aux données dont disposent déjà des autorités tierces, dans la mesure où d'autres

actes de la Confédération ne contiennent pas de dispositions contraires. Le Préposé a exigé d'une part que cet accès soit limité aux données dont l'OFS aura besoin pour accomplir ses tâches statistiques, et donc que la nouvelle procédure n'entraîne aucune extension des accès, et d'autre part que le message concernant la LMETA précise expressément que les organes fédéraux soumis à la réglementation auront l'obligation d'exclure des données accessibles toutes les données qui ne sont pas utiles à l'OFS, et notamment les données personnelles. Le Conseil fédéral devra par conséquent détailler au niveau de l'ordonnance quelles organisations devront permettre à l'OFS d'accéder en ligne à leurs données, ainsi que la nature et le domaine de provenance de ces données.

Afin de favoriser la transformation numérique de l'administration fédérale, le projet définit en outre les conditions de la réalisation de projets pilotes, notamment pour les innovations techniques. À ce propos, le Préposé a fait remarquer que les projets pilotes devront avant tout se conformer à l'art. 35 nLPD si les conditions d'application de la norme sont remplies. En dehors du champ d'application de cette norme, les projets pilotes au sens de la LMETA pourront être approuvés par le département compétent après consultation du PFPDT et d'autres services spécialisés. Le projet prévoit que les personnes concernées seront préalablement informées du projet pilote de traitement de données et invitées à donner leur consentement ; le Préposé s'en félicite.

À l'issue de la consultation, les services responsables ont tenu compte de l'intégralité des remarques formulées par le PFPDT et apporté les modifications correspondantes au projet de loi, ou se sont engagées à le faire. Le Préposé suivra attentivement la mise en œuvre des différents projets.

PROGRAMME DE GESTION NATIONALE DES DONNÉES

Le PFPDT a émis des critiques sur le relevé des données fiscales

L'Office fédéral de la statistique (OFS) a soumis au PFPDT un projet de modification de l'ordonnance sur les relevés statistiques qui prévoyait un nouveau relevé des données fiscales. Compte tenu des risques d'atteinte au droit de la protection des données que présentait ce projet, le Préposé a exigé une analyse des risques appropriée.

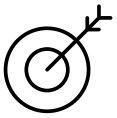
L'un des premiers projets déclinés dans le programme de gestion nationale des données (NaDB) est l'instauration d'un nouveau relevé des données fiscales par la Confédération. Le but est de permettre l'utilisation à des fins statistiques des données administratives détenues par l'Administration fédérale des contributions (AFC) et des données fiscales détenues par les administrations fiscales cantonales (conformément au principe de la collecte unique des données [cf. 28e rapport d'activités, ch. 1.1]).

En prévision de la mise en œuvre concrète du projet, l'OFS, qui dirige les travaux, a soumis à l'été 2021 aux unités administratives un projet de modification de l'annexe de l'ordonnance sur les relevés statistiques. Ce projet prévoyait notamment un nouveau relevé des données fiscales. Sur la base de ce changement, les cantons devraient une fois par an collecter toutes les données relatives à l'impôt sur le revenu et à l'impôt sur la fortune concernant les

personnes physiques, et toutes celles relatives à l'impôt sur les bénéfices et à l'impôt sur le capital concernant les personnes morales. L'AFC a été désigné organe responsable de la collecte. Les données devaient ensuite être mises à disposition de l'AFC et de l'OFS à des fins statistiques, sans être anonymisées.

Lors de la consultation des offices, le PFPDT a critiqué la procédure envisagée. Il considérait en effet qu'elle portait atteinte à la personnalité des intéressés puisque les données fiscales permettent de brosser un tableau complet de la situation d'une personne : il s'agissait de traiter, à l'avenir, de très gros volumes de données concernant chaque contribuable suisse, y compris des données sensibles relatives à la religion, à l'état de santé, à la perception de l'aide sociale, etc. L'évaluation statistique de ces données comportait en outre, selon lui, un danger de profilage, et donc un potentiel de risque important. Il estimait d'ailleurs que l'exploitation par l'AFC et par l'OFS des mêmes lots de données à des fins statistiques différentes ne ferait qu'aggraver ces risques.

Compte tenu de ces éléments, le Préposé a demandé à l'OFS de procéder au préalable à une analyse des risques appropriée, c'est-à-dire d'identifier et d'évaluer les risques et de définir des mesures pour les contrer. Il a rappelé que le principe de la finalité devait être tout particulièrement respecté dans les projets visant l'utilisation multiple de données et qu'à ce titre, l'AFC notamment devait garantir à tout moment la séparation technique et organisationnelle des données utilisées à des fins de surveillance et de celles utilisées à des fins statistiques. Il se demandait par ailleurs si les bases légales actuelles dans le domaine de la statistique fédérale sont encore conformes au principe de la légalité.



L'OFS et le PFPDT se sont entretenus à l'issue de la consultation des offices. En septembre 2021, l'OFS a indiqué au Préposé que le relevé des données fiscales ne faisait plus partie des modifications envisagées dans l'annexe de l'ordonnance sur les relevés statistiques.

APPLICATIONS DE RENCONTRES

Analyse des traitements de données

Le Préposé a poursuivi la procédure d'établissement des faits concernant une application suisse de rencontres. Au printemps 2021, le Préposé a entamé une procédure d'établissement des faits auprès du fournisseur suisse d'une application de rencontres après avoir été informé que les utilisateurs rencontraient des difficultés à obtenir que leur compte soit supprimé sur demande. Outre la clarification de ce point, la transmission de données personnelles à des tiers ainsi que le respect des exigences en matière de transparence et de sécurité des données ont également fait l'objet de notre procédure (cf. 28e rapport d'activités, ch. 1.1).

Au cours de l'année sous revue, le Préposé a établi les faits et les a transmis au fournisseur en le priant de prendre position. Ensuite, les faits ont été clarifiés avec le fournisseur et le Préposé procède maintenant à l'analyse juridique sur la base des faits constatés. Au moment de la rédaction du présent rapport, cette analyse était encore en cours.

Travaux en vue de l'entrée en vigueur de la LPD révisée

RÉVISION DE L'OLPD

Nouvelle ordonnance relative à la LPD révisée

L'élaboration de l'ordonnance relative à la nouvelle loi sur la protection des données (OLPD) va bon train. Le PFPDT a communiqué à l'Office fédéral de la justice (OFJ), qui dirige les travaux, son avis sur le projet.

Le PFPDT a reçu pour avis une première version de la future ordonnance sur la nLPD à l'été 2021. Il a depuis exposé son point de vue à diverses occasions et discuté avec l'OFJ des améliorations qui s'imposent selon lui. Il estime que certains points ne sont toujours pas réglés. Les critiques formulées lors de la procédure de consultation lui paraissant justifiées sous de nombreux aspects, il a invité l'OFJ à en tenir compte pour la suite des travaux. Les Commissions des institutions politiques des deux chambres ont elles aussi exigé des modifications à l'issue de la consultation et après l'audition du Préposé. Les travaux de révision de l'ordonnance étaient encore en cours à la fin de l'année sous revue.

Un projet trop peu détaillé

Le PFPDT estime que les dispositions d'exécution concernant l'analyse d'impact relative à la protection des données personnelles, le profilage, les décisions individuelles automatisées et les émoluments sont lacunaires et trop peu détaillées, ce qui nuira à la sécurité juridique de l'application de la loi. Il déplore surtout le quasi-silence du projet sur l'instrument clé que sera l'analyse d'impact – notamment, il n'est précisé nulle part à quel moment les organes fédéraux devront présenter une telle analyse au PFPDT. Le Préposé

Le PFPDT a publié au printemps 2021 sur son site Internet une vue d'ensemble des principales nouveautés qui figurent dans la loi révisée du 25 septembre 2020 sur la protection des données. Le Département fédéral de justice et police a annoncé que le Conseil fédéral fixerait l'entrée en vigueur de cette loi non pas au deuxième semestre 2022 comme c'était prévu initialement, mais le 1er septembre 2023.

À l'été 2021, l'Office fédéral de la justice (OFJ) a soumis un premier projet d'ordonnance d'exécution de la nouvelle LPD. Depuis lors, le PFPDT a fait part de ses exigences dans diverses prises de position. À la fin de l'année sous revue, tous les points dont le Préposé a requis l'amélioration n'avaient pas encore été pris en considération.

Parallèlement à ces projets d'accompagnement de projets législatifs, le PFPDT soutient la création de trois portails numériques qui permettront de procéder efficacement à la déclaration, prévue par la loi, des conseillers à la protection des données des entreprises, des registres des activités de traitement et des atteintes à la protection des données. Il a en outre lancé la refonte de son site internet (cf. ch. 3.2).

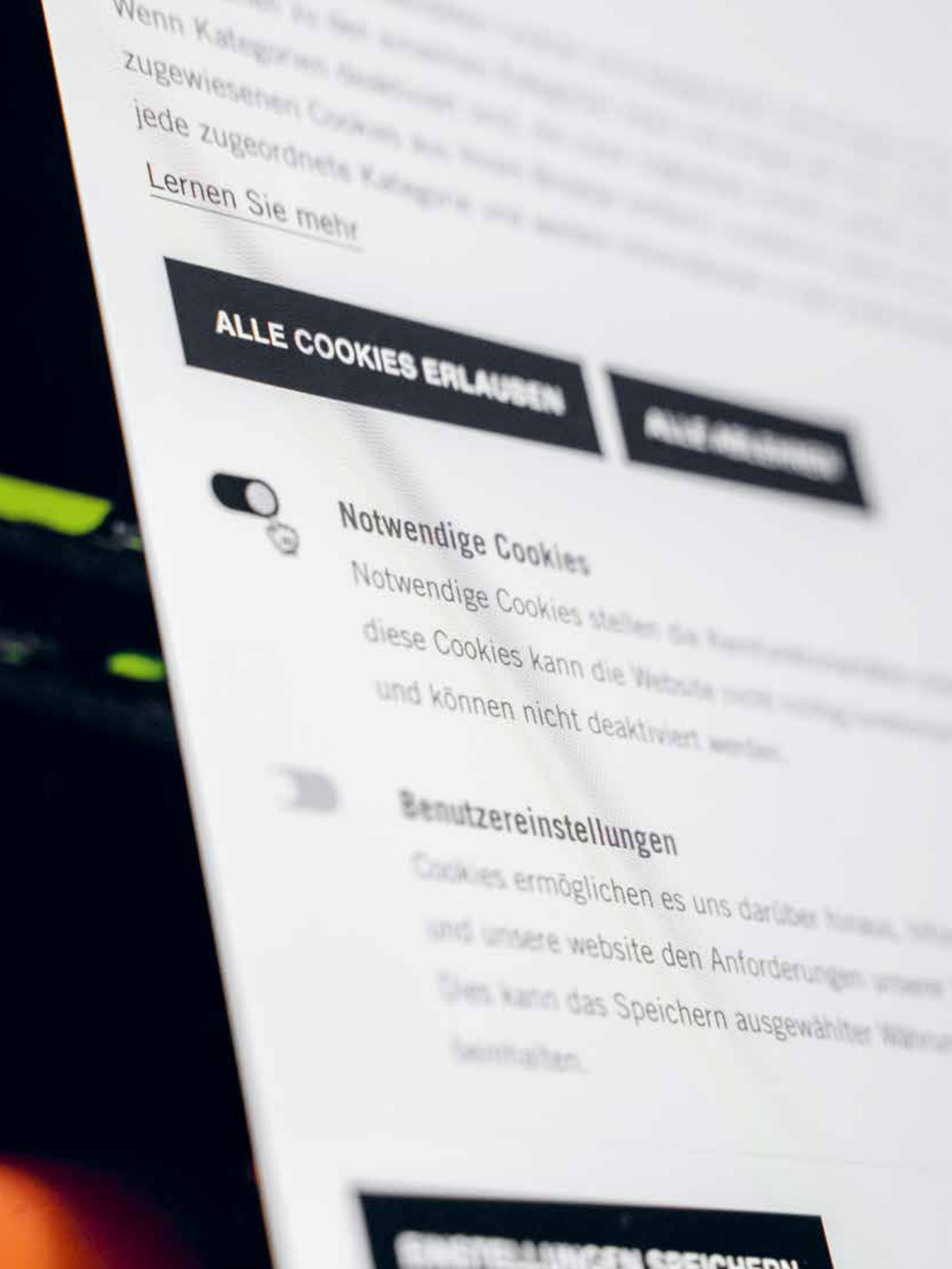
aurait par exemple souhaité que l'ordonnance prévoie que les résultats des analyses d'impact et l'avis du Préposé à leur propos figurent dans les messages destinés aux Chambres fédérales.

Bien que l'OFJ ait prévu des aides informelles à l'interprétation, l'économie et les organes fédéraux devront selon lui s'appuyer largement sur le texte de la loi, l'ordonnance restant muette sur l'accomplissement de leurs obligations de traitement. Le PFPDT en tant qu'autorité de surveillance se voit quant à lui accorder, faute de précisions dans l'ordonnance, une grande marge d'appréciation concernant l'application de la loi en vue de l'établissement d'une jurisprudence homogène et équitable, ce qui l'expose au reproche d'endosser un rôle de régulateur.

Le PFPDT a par ailleurs suggéré que soient étoffées les dispositions d'exécution relatives à l'assistance administrative, d'autant que le Conseil fédéral a déjà reconnu, dans son avis du 9 novembre 2016 sur la motion du groupe libéral-radical « Contre les doublons en matière de protection des données » (16.3752), le problème de la double surveillance exercée par le PFPDT et par les autorités étrangères de protection des données.

Renforcer le rôle des conseillers à la protection des données des offices fédéraux

Le PFPDT a accordé ces dernières années plus de poids aux responsables de la protection des données des entreprises de traitement privées en les considérant comme les premiers interlocuteurs des autorités de protection des données dans le cadre des projets de transformation numérique de l'économie privée. Le législateur a reproduit dans la révision de la loi sur la protection des données l'importance accrue de la protection des données dans les entreprises. Si l'on veut que le PFPDT continue d'assumer, sous le nouveau droit, ses tâches légales avec les ressources dont il dispose, il faut accentuer dans l'administration fédérale ce qui a déjà fait ses preuves dans le privé. Le Préposé demande par conséquent que le projet d'ordonnance accorde une importance plus grande au rôle des conseillers à la protection des données des organes fédéraux. Il lui paraît notamment indispensable que le Conseil fédéral prévoie l'obligation de consulter ces conseillers à l'avenir pour les projets législatifs de l'administration fédérale.


Wenn Kategorien
zugewiesenen Cookies
jede zugeordnete Kategorie
Lernen Sie mehr
ALLE COOKIES ERLAUBEN
Notwendige Cookies
Notwendige Cookies
diese Cookies kann die
und können nicht deaktiviert
Benutzereinstellungen
Cookies ermöglichen es uns
und unsere website den
Dies kann das Speichern

NOUVEAUX SERVICES

Portails de déclaration en ligne

En vue de la mise en œuvre de la nouvelle loi sur la protection des données (nLPD), le PFPDT proposera sur son site internet deux nouveaux portails de déclaration :

- D'une part, le portail de déclaration des violations de la sécurité des données. Il permettra aux responsables d'assumer leur obligation de notification conformément à l'art. 24 nLPD et de mettre à disposition du PFPDT les informations requises de manière sûre et rapide.

- D'autre part, le portail de déclaration des conseillers à la protection des données. Il permettra aux responsables du secteur privé et des organes fédéraux de communiquer simplement au PFPDT les renseignements nécessaires. Conformément à la nLPD, la nomination d'un tel conseiller sera facultative pour les acteurs privés et obligatoire pour les seuls organes fédéraux.

Le PFPDT procède par ailleurs à la refonte intégrale de son portail de déclaration et de consultation de fichiers appelé « Webdatareg ». Contrairement aux responsables du secteur privé, les organes fédéraux devront toujours, en vertu de la nLPD, déclarer leur registre des activités de traitement (anciennement « fichiers ») au PFPDT. Le Préposé publie ces données sur son site.

OCPD

Révision de l'OCPD

Dans le contexte de la révision totale de la loi fédérale sur la protection des données, l'ordonnance relative à la loi sur la protection des données a été remaniée, ainsi que l'ordonnance sur les certifications en matière de protection des données (OCPD). Le Préposé a accompagné les travaux relatifs au projet d'OCPD. La certification inclura désormais les services.
Outre les systèmes de traitement de données (organisation, procédure en matière de protection des données) et les produits (logiciels, systèmes pour procédures automatisées de traitement de données), la nouvelle OCPD s'appliquera aussi aux services. La certification des services permettra d'augmenter la transparence du traitement des données ou de réduire le risque de violation de la protection des données, améliorant ainsi la confiance dans les services. Les responsables certifiés en charge des traitements de données sont dispensés de l'obligation de réaliser une analyse d'impact relative à la protection des données. En effet, la certification inclut toutes les composantes du traitement de données qui auraient dû être contrôlées au moyen de cette analyse d'impact.

Le nouvel art. 6 de l'OCPD mentionne la norme ISO 27701. Cette norme est une prolongation de la norme ISO/CEI 27001 visant à couvrir la protection des données à caractère personnel et ne pouvant être mise en œuvre qu'en liaison avec cette dernière. L'ISO/CEI 27001 est une norme de sécurité des systèmes de gestion de l'information. L'ajout à cette norme de composantes relatives à la protection des données (ISO 27701) vise à renforcer la protection des données personnelles dans les offres de services au niveau mondial. La procédure de certification demeure facultative.

Le Préposé accompagne les travaux concernant l'OCPD, du point de vue juridique, informatique et technique. Nous avons des échanges avec l'OFJ et d'autres services fédéraux comme le Service d'accréditation suisse, ainsi qu'avec des organismes de certification privés.

Le projet n'était pas encore abouti lors du bouclage du présent rapport. Les indications ci-dessus correspondent à la situation à la fin de l'exercice sous revue. Le PFPDT poursuit l'accompagnement des travaux.

IDENTITÉ ÉLECTRONIQUE

Nécessité d'un système géré par l'État

En rejetant la loi fédérale sur les services d'identification électronique (LSIE) en 2021, le peuple suisse a exprimé sa volonté de faire de l'identité électronique une compétence exclusive de l'État. Le PFPDT veille à ce que la nouvelle solution soit bien conforme au droit de la protection des données et offre toutes les garanties requises au point de vue de la sûreté technique, de la facilité d'utilisation et des possibilités d'autodétermination de la population.

Après que le peuple eut rejeté la LSIE lors de la votation du 7 mars 2021, les six groupes parlementaires ont déposé au Conseil national six motions identiques détaillant leurs exigences quant à la nouvelle identité électronique (e-ID) : l'e-ID doit être un système géré par l'État qui permette de prouver son identité en ligne ; l'octroi des e-ID et le fonctionnement du système devront être assumés par des services publics spécialisés ; il faudra prendre en compte la protection de la vie privée dès la conception du produit (privacy by design), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée.

Trois pistes

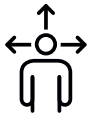
Les motions ont été acceptées et le Conseil fédéral a ensuite chargé le Département fédéral de justice et police (DFJP, représenté par l'Office fédéral de la justice [OFJ] et par l'Office fédéral de la police) d'élaborer, en collaboration avec le Département fédéral des finances, la Chancellerie fédérale, les cantons et les Écoles polytechniques fédérales, une nouvelle solution d'identification électronique qui satisfasse à ces exigences. Le DFJP a élaboré un schéma de base ouvrant trois pistes correspondant à trois niveaux d'ambition pour un écosystème e-ID :

a) une solution basée sur un fournisseur d'identité central étatique ;
b) une solution basée sur une infrastructure à clé publique, et
c) une solution basée sur une identité souveraine (SSI).

La direction du projet a tenu le PFPDT au courant de l'avancement du projet. L'OFJ a par ailleurs mené une consultation publique informelle sur le schéma de base.

L'anonymat dans l'espace public

Le PFPDT a été invité à exposer son avis sur le document de travail concernant le projet d'identité électronique (e-ID) dans le cadre d'une conférence publique. Il a déclaré que quelle que soit la solution retenue, il fallait garantir que l'e-ID ne signifie pas pour les citoyens la fin de leur anonymat dans l'espace numérique. Il a ajouté qu'il fallait que les citoyens dont le terminal



fait partie de l'infrastructure bénéficient du soutien nécessaire si des solutions décentralisées sont poursuivies, afin de pouvoir contribuer à la sécurité du système sans se voir imposer des obligations légales.

Le Conseil fédéral ayant pris une décision de principe sur l'e-ID, le DFJP est chargé d'élaborer le projet de loi d'ici au milieu de l'année 2022. Le PFPDT continuera de formuler ses exigences au fur et à mesure de l'avancement du projet.

NOUVELLES RÈGLES

Transparence du financement de la vie politique

Suite à une initiative populaire déposée en 2017, le Parlement a modifié la loi sur les droits politiques en 2021 afin d'y insérer des normes visant à assurer une certaine transparence sur le financement de la vie politique. Le PFPDT s'est déterminé sur l'ordonnance d'exécution, laquelle est actuellement en consultation externe.

À l'automne 2017, une initiative populaire intitulée « Pour plus de transparence dans le financement de la vie politique (initiative sur la transparence) » a été déposée et le Conseil fédéral a proposé son rejet en août 2018. Au cours de l'année 2019, la Commission des institutions politiques du Conseil des États a établi un rapport et écrit un contre-projet à l'initiative. En juillet 2021, l'Assemblée fédérale a modifié la loi fédérale sur les droits politiques (LDP) et adopté des normes visant à introduire une certaine transparence dans le financement de la vie politique. Les partis politiques seront ainsi contraints de publier des données, principalement celles des donateurs, relatives aux dons importants – dont le montant diffère selon qu'il s'agisse d'une élection ou une campagne de votation.

Le Contrôle fédéral des finances (CDF), autorité pressentie pour exécuter les tâches découlant des modifications de la LDP, a contacté le PFPDT dans le cadre des travaux relatifs à l'ordonnance d'exécution, puisque la loi ainsi que l'ordonnance portent sur la publication de données à caractère politique – soit potentiellement des données sensibles si elles peuvent être rattachées à une personne déterminée. En septembre 2021, une séance entre le CDF et le PFPDT a permis d'échanger des points de vue et de clarifier de nombreux points.

Requêtes du PFPDT

En novembre 2021, le projet d'ordonnance a été mis en consultation auprès des offices fédéraux. Dans ce cadre-là, le PFPDT a requis quelques précisions supplémentaires dans l'ordonnance afin d'assurer la sécurité du droit et de mieux cadrer le traitement de ces données sensibles. Ainsi, le CDF devant publier les données telles qu'il les reçoit des mouvements politiques, la notion des documents qui devront être publiés et ceux servant à procéder à des contrôles a été précisée. Il s'agissait d'éviter que des données personnelles des donateurs (par exemple leur numéro de compte bancaire) qui ne servent pas à la transparence du financement de la vie politique ne soient publiées. Enfin, une durée de cinq ans pour la publication des données a été insérée dans l'ordonnance.

La procédure de consultation externe a duré du 17 décembre 2021 au 31 mars 2022.


IC 8
12:16 Romanshorn
Winterthur Frauenfeld
SBB CFF FFS

GESTION DU SAVOIR

La Confédération développe un réseau de savoir-faire recourant à l'IA

L'Office fédéral de l'informatique et de la télécommunication (OFIT) a consulté le PFPDT sur un projet pilote visant à créer, pour l'administration fédérale, un réseau de savoir-faire recourant à l'intelligence artificielle (IA). L'idée est d'acquérir un produit utilisant un algorithme qui puisse analyser les données de l'administration fédérale de manière à diriger les questions spécialisées vers les personnes internes les plus compétentes dans le domaine concerné. Dans un premier temps, l'OFIT effectuera une analyse de l'impact qu'un tel projet pourrait avoir sur la protection des données.

L'administration fédérale utilise aujourd'hui des moteurs de recherche plein texte traditionnels. Ces derniers ne peuvent ni établir de liens entre les connaissances disponibles ni, en règle générale, effectuer de recherches contextuelles. Ils proposent uniquement une recherche lexicale qui fournit des résultats pour un ou plusieurs termes issus d'un contexte limité (par ex. un service SharePoint). Ces instruments ne permettent pas non plus la mise en relation ciblée de détenteurs de connaissances.

Contrairement aux outils de recherche et aux annuaires de personnes actuels, le réseau évalué par l'OFIT et une entreprise privée doit permettre d'identifier et de compiler les connaissances spécialisées disponibles dans l'administration de manière à les mettre à la disposition de tous les collaborateurs. Un algorithme tirera profit de l'intelligence artificielle pour mettre en relation des personnes disposant du savoir-faire requis. Cette technique permettra d'une part de traiter les questions spécialisées plus rapidement et, d'autre part, de mieux partager les expériences au sein de l'administration fédérale. Pour ce faire, au fur et à mesure qu'il reçoit des questions et des réponses déjà traitées, l'algorithme constitue une banque de profils de savoir-faire toujours plus précise. Un processus automatisé attribuera alors les questions entrantes aux collaborateurs dont le profil correspond le mieux à la matière. L'algorithme répondra lui-même aux questions qui ont déjà été traitées. Ces réponses automatiques n'auront plus qu'à être contrôlées par des collaborateurs spécialisés.

En septembre 2021, à la demande de l'OFIT, le PFPDT a rendu un premier avis sur les conditions que le projet pilote devrait respecter sur le plan de la protection des données. Il y recommande à l'office de procéder à une analyse d'impact relative à la protection des données (AIPD) pour identifier les

risques liés au traitement des données personnelles et réfléchir à des mesures qui permettraient d'y remédier. La suite des travaux, et notamment la réglementation qui encadrera le projet pilote, dépendra des résultats de cet AIPD, débuté en février 2022, et des clarifications que l'OFIT mènera en parallèle dans les domaines de la protection des informations et du droit du personnel.

1.2 Justice, police, sécurité

RÉVISION TOTALE DE LA LOI SUR LES DOUANES

Création de l'Office fédéral de la douane et de la sécurité des frontières

Le PFPDT a accompagné, en sa qualité d'expert du droit de la surveillance, les travaux d'élaboration de la loi définissant les tâches d'exécution de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) et l'analyse d'impact relative à la protection des données menée en parallèle. Lors de la troisième consultation des offices, l'OFDF a adopté d'importantes propositions d'amélioration formulées par le PFPDT.

Le Conseil fédéral a ouvert le 11 septembre 2020 la consultation sur un paquet législatif visant à créer les bases légales du programme de numérisation et de transformation DaziT de l'Administration fédérale des douanes (AFD) et dont la pièce maîtresse est la loi définissant les tâches d'exécution de l'OFDF, nouveau nom de l'AFD depuis le 1er janvier 2021.

Le PFPDT a accompagné ces travaux et l'analyse d'impact relative à la protection des données menée en parallèle, en sa qualité d'expert du droit de la surveillance. À sa demande, l'OFDF a expliqué les différences entre le projet et le droit en vigueur concernant l'ampleur et l'intensité du traitement de données personnelles. Il a de plus exposé dans l'analyse d'impact, outre les risques liés aux techniques de sécurité, les risques systémiques générés par l'attribution des tâches de la douane et du Corps des gardes-frontière de l'ex-AFD au nouveau métier de « spécialiste en douane et sécurité des frontières » et par la refonte de l'actuel bouquet d'applications en un système d'information unique.

À l'issue de la troisième consultation des offices, le PFPDT constate que le chapitre relatif au traitement des données a subi des améliorations très nettes (à propos de la première consultation des offices, cf. 27e rapport d'activités, ch. 2.4, à propos de la seconde, cf. 28e rapport d'activités, ch. 1.2). L'OFDF a aussi adopté d'importantes propositions d'amélioration formulées par le Préposé pour l'analyse d'impact relative à la protection des données. L'ampleur des divergences à éliminer n'était pas définitivement établie à la fin de la période sous revue.

RÉVISION DE LA LOI SUR LE RENSEIGNEMENT

La révision doit garantir un même niveau de transparence que la LRens actuelle

En novembre 2020, le Service de renseignement de la Confédération a informé le PFPDT d'une révision de la loi fédérale sur le renseignement (LRens) dont les buts étaient notamment l'ajout de nouvelles tâches, un nouveau concept de traitement des données et une adaptation à la nLPD. La consultation des offices en été 2021 a permis une amélioration notable du projet et les exigences du PFPDT ont été respectées. Une divergence subsiste, relative à la citation du système d'information. La procédure de consultation devrait avoir lieu au printemps 2022.

La LRens du 25 septembre 2015, entrée en vigueur le 1er septembre 2017 après une votation suite à un référendum, doit maintenant faire l'objet d'une révision totale qui vise notamment à simplifier la gestion des données conformément à un mandat de la Délégation des Commissions de gestion du Parlement.

Ce mandat a conduit à une révision du chapitre sur le traitement des données, qui a notamment consacré un changement de paradigme prévoyant le remplacement des multiples sous-systèmes de renseignement existants par un système unique.

Dans le cadre de plusieurs étapes de consultation, le PFPDT est parvenu à faire passer un grand nombre d'exigences concernant les dispositions relatives au traitement des données. Ainsi, le message relatif à la loi stipulera expressément que le futur traitement des données personnelles ne doit pas se distinguer pour l'essentiel du traitement prévu par le droit en vigueur en ce qui concerne les catégories de données et les règles d'accès. Dans le projet de loi, ces catégories de données ont été distinguées, de sorte que le traitement des données – malgré la suppression des sous-systèmes – peut toujours être attribué à des tâches spécifiques du SRC.

Il n'a cependant pas été possible de parvenir à un accord sur un point essentiel jusqu'à la fin de l'année sous revue, car le DDPS ne s'est pas laissé convaincre d'inscrire dans le projet de loi que le SRC doit en principe traiter à l'avenir toutes les données personnelles relatives au renseignement dans le système unique susmentionné. Le PFPDT rappelle que le traitement par l'ancienne police fédérale d'informations relevant du renseignement dans une multitude d'emplacements peu transparents constituait un point critique central du rapport de la commission d'enquête parlementaire du 22 novembre 1989 sur « l'affaire des fiches » de l'époque.

En revanche, il faut saluer la volonté exprimée de rapprocher le droit d'accès de la LRens à celui de la nouvelle loi sur la protection des données, renforçant ainsi les droits des personnes concernées.

Il est également positif que la volonté de soumettre la validité de la loi fédérale sur le principe de la transparence dans l'administration fédérale (LTrans) à des restrictions supplémentaires par le biais de cette révision, que nous avions critiquée, ait été abandonnée.

La consultation externe devrait commencer au deuxième trimestre 2022.

DROIT D'ACCÈS

Demandes de vérification en cas de report

Dans le cadre du droit d'accès à certaines données personnelles traitées par le Service de renseignement de la Confédération (SRC) et l'Office fédéral de la police (fedpol), la communication des renseignements peut être reportée sans indication des motifs. Le requérant peut cependant demander au Préposé de vérifier si le traitement des données est conforme au droit et si le report est justifié. Entre 2018 et 2021, le PFPDT a traité 274 demandes de vérification.

Lorsque le Préposé reçoit une demande de vérification, il envoie un accusé de réception au requérant. En même temps, il informe l'office responsable du traitement (SRC ou fedpol) de la demande de vérification. L'office concerné indique ensuite au PFPDT si le demandeur est ou non enregistré dans ses systèmes d'information.

Le demandeur n'est pas enregistré

Si le requérant n'est pas enregistré dans les systèmes d'information, l'office concerné en informe le PFPDT via une « attestation de non-enregistrement ». Le PFPDT examine alors la

demande de vérification. Si le demandeur fait valoir de manière vraisemblable qu'un report de la réponse le lèse gravement et de manière irréparable, le Préposé informe l'office concerné de son intention d'émettre une recommandation (SRC) ou une décision (fedpol), invitant à informer immédiatement le requérant qu'il n'est pas enregistré. L'office a ainsi la possibilité d'expliquer au Préposé en quoi une communication des données à la personne concernée constituerait une menace pour la sûreté intérieure ou extérieure. Si tel n'est pas le cas, l'office informe le requérant qu'il n'est pas enregistré. Suite à cela, le PFPDT envoie la communication prévue par la loi.

Cette communication, au libellé toujours identique, informe le requérant qu'aucune donnée le concernant n'a été traitée illégalement ou que le Préposé a adressé à l'office une recommandation (SRC) ou une décision (fedpol) afin de remédier à une erreur relative au traitement des données ou au report de sa réponse.

Le demandeur est enregistré

Si le requérant est enregistré dans les systèmes d'information, deux collaborateurs du Préposé se rendent dans les locaux de l'office concerné afin de vérifier la licéité du traitement des données enregistrées. Suite à cette vérification, le Préposé examine si le requérant rend vraisemblable qu'un report de la réponse le léserait gravement et de manière irréparable. Si le PFPDT parvient à la conclusion qu'un traitement de données est contraire au droit, que les conditions du report ne sont pas réalisées ou que les conditions pour une information immédiate sont réunies, il informe l'office de son intention d'émettre une recommandation (SRC) ou de rendre une décision (fedpol). L'office a alors la possibilité de présenter ses arguments. À la fin de la vérification, le PFPDT envoie la communication prévue par la loi, en tout point identique à celle décrite dans le cas de figure du demandeur non-enregistré.

Quelques chiffres

Ces quatre dernières années (2018 à 2021), le PFPDT a traité 274 demandes de vérification.

Les demandes de vérification reposant sur la loi sur le renseignement sont les plus nombreuses (180 demandes): 8 en 2018, 42 en 2019, 107 en 2020 et 23 en 2021. Les demandes basées sur la loi sur les systèmes d'information de police de la Confédération représentent une plus petite partie (93 demandes): 29 en 2018, 25 en 2019, 17 en 2020 et 22 en 2021. Nous avons reçu une seule demande de vérification en application de la loi sur l'entraide internationale en matière pénale.

SYSTÈME D'INFORMATION SCHENGEN

Activités de coordination au niveau national

Durant l'année sous revue, le PFPDT a eu des échanges permanents avec les autorités européennes et les cantons pour faire en sorte que l'on applique uniformément les dispositions du droit de la protection des données lors de l'utilisation des différentes composantes du Système d'information Schengen (SIS).

Au cours de ces dernières années, le groupe de coordination chargé de la surveillance du SIS II a constaté une augmentation des signalements destinés au contrôle discret ou au contrôle spécifique de personnes ou de véhicules dans le but de prévenir des menaces et de sauvegarder la sureté intérieure ou extérieure des États Schengen (art. 36 de la décision UE 2007/533/JAI concernant le SIS II) (cf. ch. 1.8.). C'est la raison pour laquelle il a établi un questionnaire en la matière auquel doivent répondre les autorités de protection des données des différents États Schengen. Le PFPDT a par conséquent chargé l'Office fédéral de la police (fedpol) d'analyser la licéité du traitement, en particulier de l'effacement des données dans le contexte en question, puis il a rempli le questionnaire et l'a renvoyé au secrétariat du groupe de coordination chargé de la surveillance du SIS II. Au vu de ses constatations, le PFPDT est arrivé à la conclusion qu'il n'y a pour l'instant aucune nécessité d'agir sur ce point vis-à-vis de fedpol.

Lors des réunions par visioconférence qui ont eu lieu le 1er juillet et 2 décembre 2021, le PFPDT a discuté des évolutions actuelles dans le domaine Schengen avec les représentants des autorités cantonales chargées de la protection des données dans le cadre du groupe suisse de coordination dans le domaine Schengen. Ces réunions ont aussi porté sur les expériences et les constatations faites lors de contrôles portant sur les fichiers journaux.

Dans la perspective de la prochaine évaluation Schengen auquel la Suisse sera soumise, qui est prévue pour 2023, une première réunion avec les autorités concernées a eu lieu à Berne le 8 novembre 2021. La coordination globale de l'évaluation Schengen est menée avant tout par la direction de la délégation suisse au sein du Comité Schengen, laquelle se compose de l'Office fédéral de la justice, en sa qualité de principale autorité responsable, et de la Division Europe du Secrétariat d'État du DFAE, en sa qualité d'autorité coresponsable. Les travaux sont menés au sein de neuf sous-groupes de travail, le PFPDT participant au sous-groupe de travail consacré à la protection des données. Les questionnaires seront remis aux autorités concernées dans le courant du premier semestre 2022. Les réponses seront ensuite analysées à l'issue du délai de réponse de huit semaines. Une visite sur place par les experts européens est prévue début 2023.

1.3 Commerce et économie

CRYPTOMONNAIE DIEM

Diem abandonne son projet de cryptomonnaie en Suisse

Diem Association (anciennement Libra Association) a retiré au printemps 2021 sa demande d'autorisation déposée à l'Autorité fédérale de surveillance des marchés financiers (FINMA) pour un système de paiement fondé sur la blockchain en Suisse. Le PFPDT a par conséquent arrêté ses activités de surveillance et de conseil concernant ce projet, lancées en 2019.

Diem Association (Diem), dont le siège est à Genève, est une organisation à caractère associatif qui a pour but de lancer un système de paiement fondé sur la blockchain. Le PFPDT ayant eu vent de ce projet, il a contacté Diem (à l'époque Libra Association) pour la première fois en juillet 2019. À partir de ce moment, il a entretenu des contacts réguliers avec les responsables du consortium et avec les représentants de divers organes de surveillance nationaux et internationaux (cf. 27e rapport d'activités, Accent II).

Au cours du printemps 2021, Diem a produit, à la demande du Préposé, plusieurs documents relevant du droit de la protection des données, dont des projets de programme de protection des données et une analyse d'impact des risques. Le PFPDT avait besoin de ces informations pour procéder à une évaluation technique et juridique du projet.

Alors que cette évaluation était en cours, Diem a annoncé en mai 2021 un transfert stratégique de ses activités principales de la Suisse aux États-Unis. Il prévoyait alors de lancer dans un premier temps son système de paiement des États-Unis, et de n'y rattacher que des prestataires de services financiers basés dans ce pays.

Diem a par conséquent retiré sa demande d'autorisation en Suisse déposée à la FINMA, dont le traitement avait pourtant déjà bien avancé. Le PFPDT n'étant plus compétent en la matière, il a cessé ses évaluations. Selon la presse, le projet serait près d'être abandonné aux États-Unis également.

PROCÉDURE DE SURVEILLANCE DE LA SEC

Les transmissions de données personnelles à l'autorité américaine de surveillance des marchés financiers sont en principe admises.

À la demande de la Commission américaine des opérations boursières (United States Securities and Exchange Commission SEC), le Préposé a examiné si les entreprises suisses, au cas où elles sont enregistrées auprès de la SEC, peuvent lui transmettre les données requises par le droit américain dans le cadre d'une procédure de surveillance de la SEC sans contrevenir à la loi suisse sur la protection des données. La réponse est en principe affirmative. Le Préposé a remis une prise de position à ce sujet. La question de la transmission de données personnelles protégées par le droit pénal reste ouverte.

Au cours de l'année sous revue, la SEC a contacté le Préposé fédéral à la protection des données et à la transparence pour savoir si, au cas où elles sont enregistrées auprès de la SEC, les entreprises suisses peuvent transmettre à celle-ci les données personnelles requises par le droit américain sans enfreindre la loi suisse sur la protection des données (LPD). Jusqu'à présent, la SEC n'autorisait pas les entreprises suisses à s'enregistrer car elle craignait que dans une éventuelle procédure de surveillance, celles-ci ne transmettent pas les données requises.

Le Préposé a pris position sur cette question après réception des documents nécessaires. Sa conclusion est la suivante : en l'absence d'un niveau de protection des données adéquat aux États-Unis, les entreprises suisses

peuvent transmettre des données personnelles à la SEC uniquement si l'un des motifs justificatifs mentionnés à l'art. 6, al. 2, LPD pour les transmissions de données à l'étranger est rempli. Plusieurs de ces motifs justificatifs entrent en ligne de compte en vue d'une transmission de données à la SEC.

En premier lieu, une transmission de données à la SEC se justifie souvent par le fait qu'il s'agit d'un traitement de données en relation directe avec la conclusion ou l'exécution d'un contrat (art. 6, al. 2, let. c, LPD). Un intérêt public prépondérant (art. 6, al. 2, let. d, LPD) ou le consentement de la personne concernée (art. 6, al. 2, let. b, LPD) entrent également en ligne de compte comme motif justificatif possible d'un transfert de données.

Le Préposé n'a pas pris expressément position sur la question de savoir si ou à quelles conditions les données personnelles régies non seulement par la LPD, mais aussi par le droit pénal (notamment les données soumises au secret bancaire) peuvent être transmises à la SEC. Le Préposé n'a pas de compétence pour interpréter le code pénal suisse ou d'autres lois pertinentes. Cette prise de position est publiée en anglais sur le site du Préposé. La SEC ne nous a pas informés plus en détail sur les conséquences qui en découlent pour l'admission des entreprises suisses à l'enregistrement.

BOUTIQUE EN LIGNE

Traitement de données clients

Dans le cadre d'un établissement des faits mené auprès d'une des plus grandes boutiques en ligne de Suisse, le Préposé a clarifié les questions ouvertes et les imprécisions en lien avec l'exploitation des données clients.

Au printemps 2021, le Préposé a entamé une procédure auprès de l'une des plus grandes boutiques en ligne de Suisse afin de vérifier si l'entreprise traitait les données de ses clients conformément au droit de la protection des données. Il a entre autres examiné la manière dont l'exploitant de la boutique en ligne traitait les demandes d'oppositions des clients.

Après avoir constaté, au cours des clarifications préliminaires, que l'exploitant rejetterait les oppositions à certains traitements de données, en particulier celles liées à l'enregistrement et à l'analyse du comportement d'achat sous forme personnalisée, le Préposé a concentré son enquête sur la question de savoir si ces traitements pouvaient être effectués contre la volonté expresse des clients (cf. 28e rapport d'activités, ch. 1.4).

Au cours de l'année sous revue, le PFPDT a analysé les traitements de données en cause et interrogé l'exploitant. Il a ainsi clarifié les faits en date du 26 janvier 2022 et, sur cette base, entamé l'analyse juridique du cas. Celle-ci était encore en cours lors de la rédaction du présent rapport.

SWISS MARKETPLACE GROUP

Plateforme de vente aux enchères Ricardo : du nouveau dans la procédure

La procédure lancée en 2017 contre Ricardo et TX Group à propos de l'utilisation de données collectées sur la plateforme de vente aux enchères en ligne ricardo.ch a connu de nouveaux rebondissements pendant l'année sous revue.

Depuis 2017, le PFPDT fait chaque année le point sur la procédure d'établissement des faits lancée contre Ricardo et TX Group. Selon son appréciation juridique des faits, il faut que le profilage établi par TX Group à partir de données provenant de différentes sources aux fins de ciblage publicitaire soit clairement visible pour les personnes concernées, dont il nécessite par ailleurs le consentement explicite (cf. 28e rapport d'activités, ch. 1.4).

Entre-temps, Ricardo et TX Group ont procédé sur leurs plateformes à d'importantes modifications et adaptations. Le PFPDT s'est particulièrement intéressé à leurs nouvelles plateformes de gestion du consentement. Il a aussi examiné l'évaluation de l'intérêt légitime qui lui a été présentée en août 2021, dans laquelle TX Group conclut que l'utilisation des données de Ricardo et le profilage en vue d'un ciblage publicitaire correspondent à un intérêt légitime prépondérant qui lui permet de se passer du consentement des intéressés.

Fin novembre 2021, TX Group nous a par ailleurs indiqué que les entreprises TX Group SA, Ringier SA, la Mobilière et General Atlantic avaient lancé le 11 du même mois une coentreprise de plateformes numériques baptisée SMG Swiss Marketplace Group, dont Ricardo SA fait partie avec ses offres et ses portails. Le PFPDT s'est alors mis à vérifier l'influence de ces changements techniques et organisationnels sur les traitements de données concernés par la procédure en cours. Ces clarifications étaient encore en cours lors du bouclage du présent rapport.

VÉRIFICATION DE LA CAPACITÉ À CONTRACTER UN CRÉDIT

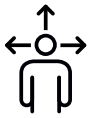
Clarifications auprès d'un fournisseur de leasing automobile

Le PFPDT a clos, sans prendre de mesures formelles, les clarifications entreprises au cours de la précédente année auprès d'un grand fournisseur de leasing automobile. Celles-ci portaient sur le traitement des données lors de l'évaluation de la capacité des clients à contracter un crédit. Le fournisseur de leasing a assuré qu'il appliquerait les deux propositions d'amélioration relatives au consentement.

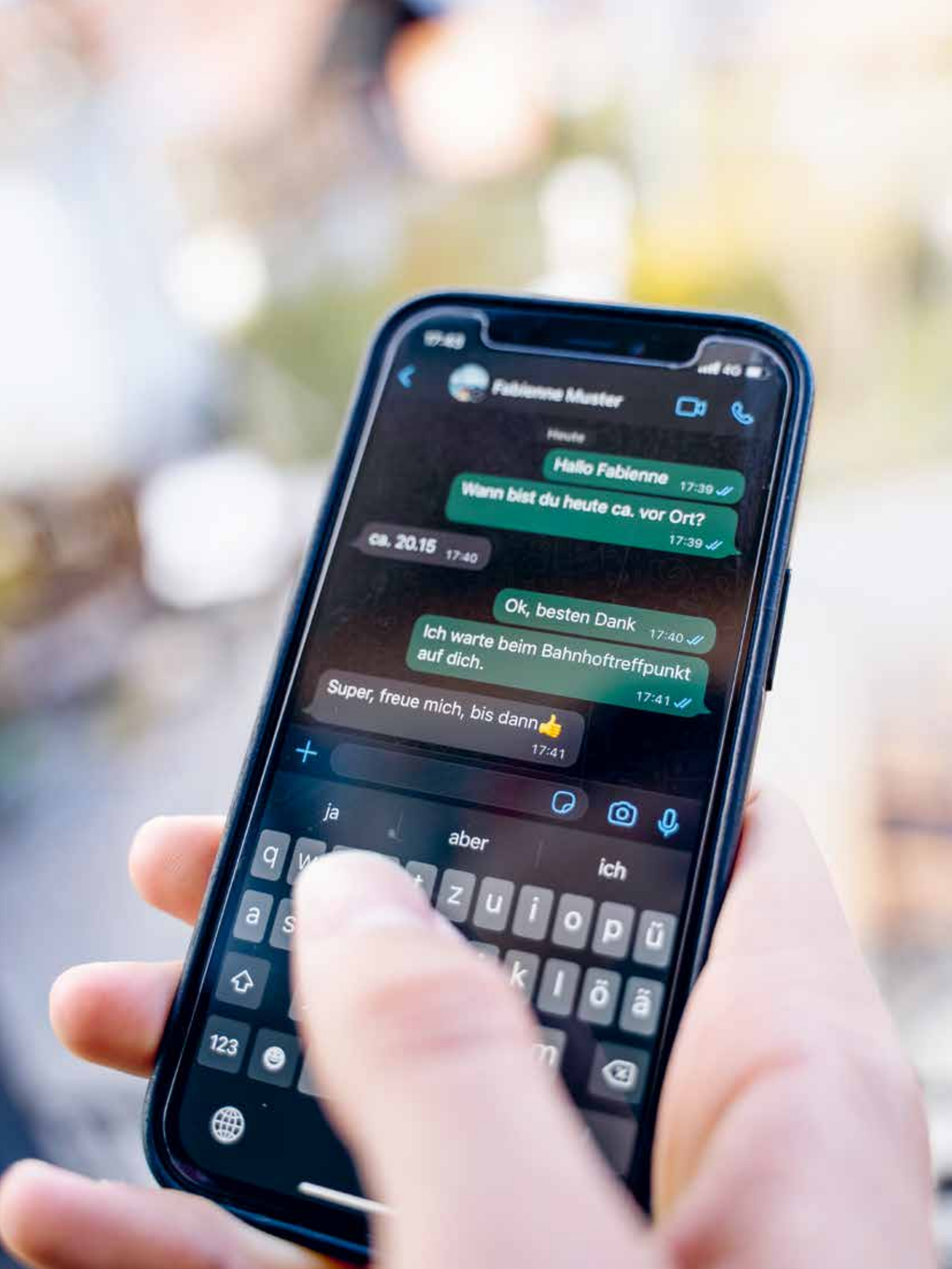
Les clients désireux de conclure un contrat de leasing pour acheter une voiture doivent donner leur consentement pour que le fournisseur de leasing vérifie leur solvabilité. Dans le cadre d'une demande citoyenne, le Préposé a été rendu attentif au fait qu'un fournisseur réclamait – dans le but de vérifier la solvabilité de ses preneurs de leasing – un consentement lui permettant d'obtenir de nombreuses informations auprès de tiers, tels que le conjoint ou les membres de la famille.

Par conséquent, le Préposé avait entrepris les premières démarches en décembre 2020 afin de déterminer si ces traitements de données respectaient le niveau autorisé par la loi (cf. 28e rapport d'activités, ch. 1.4). Après examen de la réponse du fournisseur de leasing, le Préposé est arrivé à la conclusion que le traitement des données destiné à déterminer la solvabilité des preneurs de leasing devrait être, dans une large mesure, conforme aux dispositions relatives à la protection des données.

Toutefois, le Préposé a exprimé certaines réserves concernant le traitement de données relatives au partenaire vivant dans le même ménage que le preneur. D'une part, dans le cas où le fournisseur de leasing voudrait justifier le traitement des données du partenaire en se basant sur le consentement de ce dernier, le Préposé a recommandé de recueillir sa signature ou une déclaration de consentement.



D'autre part, le Préposé a contesté la levée prétendument irrévocable du blocage de la communication des données auprès des offices de poursuites, de la ZEK, de l'IKO et de la Poste suisse. Le Préposé a attiré l'attention de la société sur le fait qu'un consentement relatif à la protection des données peut à tout moment, de manière informelle et sans justification, être révoqué. Par conséquent, la clause figurant dans le formulaire de consentement selon laquelle la levée du blocage de la communication des données est considérée comme « irrévocable » doit être supprimée. La société de leasing a assuré qu'elle appliquerait ces deux mesures.


Fabienne Muster
Heute
Hallo Fabienne 17:39
Wann bist du heute ca. vor Ort? 17:39
ca. 20.15 17:40
Ok, besten Dank 17:40
Ich warte beim Bahnhoftreffpunkt auf dich. 17:41
Super, freue mich, bis dann 17:41
ja
aber
ich

MITTO AG

Enquête sur l'éventuelle utilisation abusive de l'accès au Signalling System

Un article paru dans la presse le 6 décembre 2021 a lancé de graves accusations contre un collaborateur de la société Mitto AG, dont le siège est à Zoug. Cette société, spécialisée dans l'envoi de SMS pour de gros clients dans le monde entier, aurait permis à des tiers de surveiller en parallèle certaines personnes de manière illicite et contre rémunération.

Le Bureau of Investigative Journalism, une organisation à but non lucratif basée à Londres, et l'agence de presse Bloomberg ont publié une enquête révélant qu'un collaborateur de la société zougoise Mitto AG aurait fait un usage abusif de l'accès accordé par les opérateurs de téléphonie mobile à leurs réseaux pour l'envoi de SMS en masse, à savoir l'obtention d'informations. Ainsi, selon l'article en question, il aurait utilisé l'accès au protocole de signalisation SS7 pour permettre à des tiers de surveiller certaines personnes de manière illicite, et cela contre rémunération.

Le 7 décembre 2021, le Préposé a ouvert une enquête préliminaire concernant cette affaire. Dans un premier temps, il a demandé à Mitto AG de prendre position et a également contacté les opérateurs de téléphonie mobile en Suisse. Ces derniers ont confirmé la réalité d'une collaboration avec Mitto AG, mais ont précisé qu'il existait suffisamment de mesures techniques de protection pour empêcher les accès illicites aux données personnelles. Sur la base de ces premières réactions, le Préposé ne dispose donc à ce stade d'aucun indice lui permettant de conclure qu'il y aurait eu des abus au détriment de la population suisse.

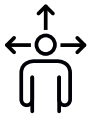
La société Mitto AG a répondu au Préposé qu'elle n'avait pas connaissance d'une telle éventualité. Elle l'a également renseigné, à sa demande, sur les mesures techniques et organisationnelles mises en œuvre pour protéger les données personnelles. Le Préposé examine actuellement ces documents afin de déterminer si des manquements ont été constatés dans les activités de Mitto AG en ce qui concerne les mécanismes de contrôle et l'attribution d'autorisations aux collaborateurs. Cet examen était encore en cours au moment de la clôture de la rédaction.

MEDIAS SOCIAUX

Les nouvelles conditions d'utilisation de WhatsApp sensibilisent à la protection des données

En janvier 2021, l'application de messagerie instantanée WhatsApp a informé ses utilisateurs d'une modification imminente de ses conditions d'utilisation et de sa politique de confidentialité. À cette occasion, l'acceptation des nouvelles conditions a été déclarée obligatoire pour les personnes désirant continuer à utiliser WhatsApp. Le Préposé a examiné les modifications en cause et a répondu aux questions de citoyens et de journalistes inquiets à ce sujet.

On entend souvent dire que la plupart des gens sont prêts à partager sans hésitation leurs données personnelles en échange de services gratuits. Toutefois, la situation s'est avérée bien différente lorsque WhatsApp a annoncé l'introduction de nouvelles conditions d'utilisation. Très vite, des citoyens inquiets se sont adressés au Préposé pour lui faire part de leurs préoccupations. Redoutant de perdre le contrôle de leurs propres données, ils étaient peu enclins à accepter ces nouvelles conditions et se sont rendus compte à quel point ils étaient dépendants de WhatsApp



lorsque certains parmi leurs proches ou amis n'étaient pas disposés à changer de messagerie. Le Préposé a donc analysé de plus près les nouvelles conditions d'utilisation et la nouvelle politique de confidentialité de WhatsApp.

Selon toute apparence, l'incertitude des utilisateurs de WhatsApp était due au fait qu'il existait désormais deux versions différentes des conditions d'utilisation et des directives de protection des données : l'une pour l'espace européen (dont fait partie la Suisse) et l'autre pour le reste du monde. Les changements étaient effectivement plus importants pour la seconde : ainsi, le groupe Meta (auparavant Facebook) s'accorde désormais le droit de lier encore plus étroitement les données de ses différentes entités (WhatsApp, Instagram et Facebook) et de les utiliser aussi à des fins de marketing ou de les partager avec des entités tierces. Cela ne concerne pas le contenu des messages ou des appels, chiffrés de bout en bout et demeurant donc inexploitables, mais uniquement les données secondaires, dont la collecte et l'analyse permettent néanmoins à Meta de tirer différentes conclusions sur les utilisateurs : à quelle fréquence interagissent-ils avec un groupe ou une personne, quels sont leurs intérêts en fonction des groupes auxquels ils appartiennent, etc.

Peu de changements pour les utilisateurs en Suisse

En revanche, selon les clarifications menées par le Préposé, les conditions d'utilisation pour les résidents de la région européenne (Suisse comprise) n'ont guère été modifiées. Les principaux changements concernaient des adaptations linguistiques telles que des précisions (p. ex. informations sur les métadonnées des messages ou sur la collaboration avec d'autres structures du groupe Meta) ou des compléments (p. ex. concernant la base juridique des traitements de données, les relations avec les utilisateurs qui enfreignent les conditions d'utilisation ou les données conservées). Les seules dispositions nouvelles étaient celles précisant quelles données pourraient être traitées à l'avenir lorsqu'une personne privée contacte une entreprise par le biais du nouveau WhatsApp Business. En revanche, rien ne change pour les personnes sans interaction avec les comptes professionnels WhatsApp. Telle a été la réponse du Préposé aux questions des particuliers et des médias.

Même si la plupart des craintes des utilisateurs suisses se sont avérées infondées, les discussions autour des nouvelles conditions d'utilisation de WhatsApp ont incité de nombreux citoyens à reconsidérer l'utilisation de services gratuits. Ils ont ainsi pris conscience que nombre de ces offres reposent sur des modèles économiques axés sur la monétisation des données et qu'il est important de lire plus attentivement les conditions générales et les déclarations de confidentialité. Nous le recommandons non seulement lors de l'utilisation de services gratuits, mais aussi, indépendamment du modèle de tarification, lors de la conclusion de contrats avec des prestataires de services, car il peut arriver, même si les services sont payants, que des données de clients soient traitées pour les besoins propres du fournisseur.

Le Préposé constate qu'il n'y a guère plus de transparence quand les conditions générales et dispositions de protection des données sont certes formulées dans les détails, mais de manière peu compréhensible pour le profane. Dans ce contexte, et dans le cadre de son activité de conseil et de surveillance, il s'efforce de promouvoir la qualité des informations mises à la disposition des utilisateurs.

ONELOG

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

Pendant l'année sous revue, le PFPDT a suivi l'avancement du projet d'authentification unique pour les plateformes de l'Alliance numérique suisse.

Le projet d'authentification unique pour les plateformes de l'Alliance numérique suisse (cf. 28e rapport d'activités, ch. 1.1.) a progressé pendant l'année sous revue. Les médias concernés ont créé la coentreprise de traitement de données OneLog, qui centralise la gestion du single sign on (SSO). Les suggestions d'amélioration formulées par le PFPDT ont été prises en compte et transposées dans des mesures techniques et dans l'organisation. Il est par exemple exclu que les membres de l'alliance utilisent OneLog pour échanger et mettre en relation des données personnelles en vue d'obtenir sur les utilisateurs des informations collectées par d'autres membres.

OneLog a aussi élaboré des processus et des règlements qui garantissent la protection des données et qui permettent aux utilisateurs de faire valoir leurs droits (à l'information, à la suppression et à la correction, notamment). Elle exige par ailleurs des membres de l'alliance, par contrat, qu'ils utilisent le SSO conformément au droit de la protection des données. OneLog a désigné un responsable interne de la protection des données chargé de veiller au respect de ce droit dans l'ensemble du système.

Le SSO a été lancé à la fin de l'été 2021 et adopté depuis par plusieurs médias. Le PFPDT continue de suivre son évolution.

PUBLICITÉ DES COMPTES POSTFINANCE

Insertion automatique des coordonnées des titulaires de compte

Un particulier a signalé au PFPDT que l'e-banking de PostFinance permettait de consulter les coordonnées d'un nombre illimité de titulaires de compte. Depuis lors, la Poste a restreint l'insertion automatique des données de compte à des proportions raisonnables par des mesures appropriées. Le PFPDT exige par ailleurs que les clients aient la possibilité de s'opposer à la publicité des comptes.

Tant que le Suisse moyen effectuait l'essentiel de ses versements en espèces au guichet de la poste, les coordonnées du destinataire du paiement étaient vérifiées manuellement. On se référait à un registre public sur lequel étaient référencés les nom et adresse de tous les titulaires d'un compte postal. Ce registre a été intégré il y a quelques années au système d'e-banking de PostFinance : dès qu'on saisit un numéro de compte PostFinance dans la fenêtre de saisie d'un paiement, le système y ajoute automatiquement le nom et l'adresse du titulaire du compte. Cette fonction, qui permet de minimiser les erreurs de saisie, contribue toujours au bon déroulement des opérations de paiement. Elle est limitée aux comptes PostFinance, et les clients en sont informés dans les conditions générales de la banque et dans une notice spécifique sur la publicité des comptes.

Selon le particulier qui a contacté le Préposé, l'e-banking de PostFinance permettait de saisir un nombre illimité de comptes. On pouvait donc, en saisissant des numéros au hasard, effectuer une recherche de masse pour faire surgir les nom et adresse des titulaires.

PostFinance a assuré au Préposé que la limitation prévue initialement avait été désactivée par inadvertance, ce qui a ouvert la voie à ces recherches de masse pendant environ deux ans. Le particulier ayant aussi contacté directement PostFinance, la limitation (10 recherches maximum par 24 heures) a été réactivée.

Le PFPDT estime que l'insertion automatique des coordonnées du titulaire d'un compte est utile et que les clients de PostFinance en sont correctement informés. Il considère que la réactivation de la limitation a réduit le risque de recherche de masse à un niveau raisonnable, mais qu'étant donné que la fonction en question n'est pas obligatoire pour l'exécution des paiements et repose en fin de compte sur le consentement des intéressés, il faudrait laisser aux clients la possibilité de s'opposer à une telle utilisation de leurs données. Le PFPDT a donc invité PostFinance à intégrer une possibilité d'opt-out au système.

RENSEIGNEMENTS SUR LA SOLVABILITÉ

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

Dans le cadre de la procédure d'établissement des faits en cours concernant d'éventuelles entrées incorrectes dans les banques de données de l'une des principales sociétés de recouvrement collectant des renseignements sur la solvabilité, le Préposé a obtenu de nouvelles informations, au sujet notamment de la « confusion de solvabilité négative dans un ménage ».

Comme l'indique notre précédent rapport d'activité, en février 2020, le Préposé avait engagé une procédure d'établissement des faits auprès d'une grande société de recouvrement en raison d'écritures supposément incorrectes dans sa banque de données, de la confusion qui en était résultée entre des personnes ayant des noms ou des adresses identiques ou similaires, ainsi qu'en raison des difficultés éventuelles à corriger ces entrées incorrectes (cf. 28e rapport d'activités, ch. 1.4).

À la suite de questions émanant de médias et de citoyens, le Préposé avait dans un deuxième temps élargi son enquête à la question de la « solvabilité négative dans un ménage ». Cela désigne le fait que, dans le cadre d'un contrôle de solvabilité, des entrées négatives d'autres personnes du même ménage sont communiquées aux vendeurs en ligne (cf. 28e rapport d'activités, ch. 1.4). Le but est d'empêcher que des personnes ayant une note de solvabilité négative puissent passer commande sur facture au nom d'une personne du même ménage ayant une note de solvabilité positive.

Le traitement de données sur la solvabilité négative soulève diverses questions concernant la protection des données, raison pour laquelle le Préposé a demandé davantage d'informations à la société. Ces informations font actuellement l'objet d'un examen. Le Préposé déterminera la marche à suivre en fonction des résultats.

ASSOCIATIONS

Nouvelle carte de membre avec carte de crédit intégrée

La Fédération sportive suisse de tir (FST) a envoyé à plus de 50 000 tireurs licenciés une nouvelle carte de membre comportant une fonction de carte de crédit. Nombreux ont été les membres de la FST à exprimer leur mécontentement face à cette commercialisation de leurs données. À la suite d'échanges avec la FST, le Préposé a obtenu que les données personnelles des membres de la fédération soient traitées dans le respect des principes de la protection des données.

L'envoi de plus de 50 000 nouvelles cartes de membre avec fonction de paiement intégrée a suscité de nombreuses questions de la part des membres de la FST quant à la protection de leurs données personnelles. Dans un premier temps, le Préposé a demandé à la fédération de lui fournir des informations supplémentaires sur l'utilisation de ces données.

Certes, la FST avait déjà confié ces dernières années l'émission de sa carte de membre à une entreprise externe. Mais, dans le cas de ce mandat, le nouveau fournisseur de cartes de crédit poursuit également ses propres objectifs et a accès à de nouveaux clients. La transmission des données des membres au fournisseur de cartes de crédit est donc une communication de données qui doit répondre aux principes de traitement de la loi sur la protection des données, tout particulièrement les principes de finalité et de transparence.

Les données personnelles ne peuvent être traitées que pour atteindre la finalité qui a été communiquée lors de leur collecte, qui découle des circonstances ou qui est prévue par la loi. Depuis 2016, les statuts de la FST prévoient la communication des données de ses membres à des fins commerciales mais aussi la possibilité de s'opposer à cette communication. La FST a donc en principe préparé le terrain pour l'utilisation commerciale des données de ses membres.

Cependant, le fait que ces informations ne figurent explicitement que dans les statuts de la FST pose un problème. Pour la plupart, les statuts des 36 fédérations régionales et des plus de 2000 sociétés de tir ne contiennent pas de réglementation analogue, mais renvoient d'une manière générale aux statuts de la FST. De ce fait, il est très difficile pour les membres des sociétés de tir d'avoir connaissance de ces informations et de s'opposer à la communication de leurs données. Le Préposé a constaté en outre que la communication des données de la FST au fournisseur de cartes de crédit ne répondait pas à l'obligation de transparence établie par le droit de la protection des données. Celui-ci dispose que les finalités du traitement doivent être reconnaissables pour la personne concernée.

En accord avec la FST, il a été convenu que les membres seraient à nouveau informés par la fédération – via son site Internet, sa newsletter et son journal – de la communication de leurs données personnelles à des fins commerciales et qu'ils pourraient faire usage de leur droit d'opposition par une simple notification à la fédération.

La FST a dû ensuite s'assurer que le fournisseur de cartes de crédit traite séparément les données des membres ne souhaitant qu'une carte de membre et non une carte de crédit, et ne les utilise pas à ses propres fins, par exemple des activités de marketing ou de promotion. Les personnes refusant la carte de crédit intégrée à la carte de membre pourront continuer à s'identifier lors des manifestations en indiquant leur numéro de membre et en présentant un document d'identité.

1.4 Santé

CORONAVIRUS

Accompagnement du projet pour un certificat COVID-19 conforme à la protection des données et « certificat light »

Le PFPDT a participé, à titre consultatif, aux réunions du groupe de projet mis en place par l'Office fédéral de la santé publique pour développer un certificat COVID-19 uniforme, infalsifiable et reconnu au niveau international. Dans cette fonction, il a insisté sur la création du « certificat light », ne contenant que les données strictement nécessaires.

Pour faire face à la pandémie, la Suisse a mis en place au début du printemps 2021 le certificat COVID-19. Celui-ci sert à prouver que son titulaire est vacciné contre la maladie, qu'il en est guéri ou qu'il a subi récemment un test de dépistage négatif. La base du certificat est inscrite à l'art. 6a de la loi COVID-19. Dans le cadre de son obligation de conseil, le PFPDT s'est engagé au sein du groupe de projet mis en place par l'Office fédéral de la santé publique (OFSP) pour une mise en œuvre du mandat législatif conforme à la protection des données. Le document devait par conséquent être personnel, infalsifiable et, dans le respect de la protection des données, vérifiable ; il devait être conçu de manière que seule une vérification décentralisée ou locale de son authenticité et de sa validité soit possible. Enfin il devait, dans la mesure du possible, être utilisé par son détenteur pour entrer dans d'autres pays et en sortir. Par ailleurs, le PFPDT a d'emblée exigé que l'introduction du certificat ne se transforme pas en obligation générale d'avoir son téléphone portable sur soi. C'est pour cette raison que le certificat COVID-19 peut être utilisé sous forme papier et sous forme numérique.

Certificat light ne contenant qu'un minimum de données

L'Office fédéral de l'informatique et de la télécommunication (OFIT) a développé un certificat compatible avec le certificat de l'UE permettant le trafic transfrontalier des personnes. Le PFPDT a réussi à faire en sorte qu'il développe également un deuxième code QR traitant beaucoup moins de données pour une utilisation en Suisse uniquement : le certificat light. Celui-ci peut être généré dans l'application COVID Certificate et ne précise pas si le certificat a été obtenu à la suite d'une vaccination, d'une guérison ou d'un test. Pour éviter toute déduction sur la raison d'émission, le certificat light, valable uniquement sur le territoire national, a une durée de validité très courte au terme de laquelle il doit être généré une nouvelle fois.

Ainsi, le certificat light contient uniquement les données d'identification indispensables et une signature électronique, de sorte qu'il n'y a pas de risque qu'une personne utilisant une application de vérification autre que celle de la Confédération puisse accéder indûment aux données de santé du certificat. Lors du contrôle d'accès à une manifestation, il n'est en effet souvent pas nécessaire de savoir la raison pour laquelle un visiteur a obtenu son certificat.

Problème de la règle des 2G

L'évolution de la pandémie a poussé le Conseil fédéral en décembre 2021 à restreindre l'accès à certains lieux et à certaines manifestations aux seules personnes guéries ou vaccinées. Un résultat de test négatif n'était dès lors plus suffisant. Ces règles dites des 2G ou 2G+ ne permettaient plus l'utilisation du certificat light, étant donné qu'il était conçu pour ne pas dévoiler le


13:31
COVID-ZERTIFIKAT

statut (vacciné, guéri ou testé). Il s'agissait d'une limitation ni planifiée ni prévisible au moment où le système avait été développé. Afin de pouvoir utiliser le certificat light sous le régime 2G ou dans d'autres contextes spécifiques, il faudrait soit établir des certificats différents (2G+, 2G et 3G), soit intégrer des informations sur le statut d'autorisation directement dans le certificat. La seconde possibilité aurait pour conséquence d'ajouter une donnée de santé au certificat light, ce qui irait à l'encontre de l'intention initiale. Quelque soit la solution retenue, le PFPDT a exigé que le certificat light puisse à nouveau être pleinement utilisé en cas de retour à la règle des 3G.

Emploi proportionné du certificat

Le PFPDT a veillé à la création d'un certificat conforme à la protection des données et à son développement technique. Il a aussi fait en sorte que son utilisation ne soit pas laissée au bon vouloir de personnes et institutions privées mais qu'elle soit encadrée par des règles de droit public.

Les conditions d'utilisation ont été inscrites dans l'ordonnance COVID-19 situation particulière (RS 818.101.26). Après que le certificat est devenu obligatoire dans un premier temps pour les grandes manifestations, son utilisation s'est étendue en plusieurs étapes à d'autres domaines tels que les restaurants, les bars et les lieux de loisir (musées, bibliothèques, zoos, centres de sport, piscines couvertes ou casinos). Le PFPDT a souligné à plusieurs reprises dans le cadre de consultations des offices à très court terme que les restrictions d'accès sur la base d'un certificat, et donc le traitement des données de santé qui y sont liées, pouvaient être considérées comme proportionnées sur le plan de la protection des données, uniquement si ces mesures étaient nécessaires et appropriées d'un point de vue épidémiologique pour lutter contre la pandémie. Il incombe à l'OFSP, en tant qu'office compétent, d'en apporter la preuve, raison pour laquelle le PFPDT s'est toujours appuyé sur ses constatations et ses évaluations pour émettre ses avis.

En ce qui concerne notamment la possibilité d'imposer le certificat sur le lieu de travail, le PFPDT a défendu le point de vue selon lequel les employeurs ne peuvent exiger un tel certificat dans le cadre de leur devoir d'assistance qu'après avoir soigneusement pesé les intérêts en jeu et uniquement en relation avec la mise en place de mesures de protection concrètes ou d'un plan de dépistage.

TRAÇAGE DES CONTACTS

Établissement des faits concernant l'application SocialPass

Dans le cadre d'une procédure d'établissement des faits, le Préposé a examiné l'application privée SocialPass dont le but était de saisir les données des clients de restaurants et des visiteurs d'événements. Dans son rapport final, le Préposé a notamment recommandé aux exploitants de l'application d'améliorer la sécurité technique de celle-ci et de limiter de manière proportionnée l'accès des autorités sanitaires cantonales aux données enregistrées de manière centralisée. Après les avoir contestées dans un premier temps, les exploitants ont accepté de mettre en œuvre les principales recommandations du Préposé.

Dans le cadre de la lutte contre la pandémie, dès l'été 2020, les restaurateurs et les organisateurs d'événements ont été tenus de relever les coordonnées de leurs clients pour pouvoir les transmettre plus tard aux autorités sanitaires cantonales si une infection de COVID-19 était notifiée, et cela à des fins de traçage des contacts.

L'application SocialPass, exploitée conjointement par deux entreprises privées établies en Suisse, permettait aux utilisateurs d'enregistrer aisément leurs données au moyen d'un smartphone. Sur la base de diverses informations fournies par la population, des doutes sont toutefois apparus quant à la conformité de l'application avec la protection des données, si bien qu'en décembre 2020, le Préposé a ouvert une procédure formelle afin de faire la lumière sur ces critiques également relayées par les médias. Dans son rapport final, le Préposé a constaté de nombreuses lacunes qui ont conduit à un total de dix recommandations. Après plusieurs visioconférences auxquelles ont aussi participé les autorités sanitaires des cantons de Vaud et du Valais, les exploitants de l'application ont accepté la plupart de ces recommandations.

Principales recommandations du Préposé et mise en œuvre

Outre la constatation d'insuffisances organisationnelles et techniques, l'établissement des faits a révélé que les exploitants privés avaient accordé aux autorités sanitaires des cantons de Vaud et du Valais un accès direct à la banque de données centrale et leur avaient ainsi permis de la consulter à leur convenance malgré l'absence de motifs justificatifs, et en violation du principe de proportionnalité. Selon les médias, les possibilités de consultation accordées dans le canton du Valais auraient même conduit à des traitements de données personnelles contraires à l'objectif visé. Sur recommandation du Préposé, les exploitants ont fini par reconnaître ces insuffisances, qu'ils avaient initialement contestées, et ont déclaré y avoir depuis remédié.

Une procédure inhabituellement longue et difficile

SocialPass était une application privée, utilisée dans toute la Suisse, traitant des données personnelles dans le but de lutter contre la pandémie. Dans ce contexte, le Préposé a été tenu de suivre de près l'évolution de la situation épidémiologique afin de faire aboutir à temps la procédure d'établissement des faits. Toutefois, cette procédure s'est avérée particulièrement longue et laborieuse. Lors de la fixation des délais de réponse et au cours de l'examen des nombreuses demandes de leur prolongation et même de récusation des collaborateurs du Préposé en charge du dossier, ce dernier a dû tenir

compte du fait que vers le début de l'été 2021, la deuxième vague baissait. La réouverture des restaurants était alors prévisible et la réutilisation de l'application SocialPass imminente.

Pour les raisons susmentionnées, le Préposé a dû veiller, dans la présente procédure, à informer la population en temps utile des possibilités techniques de SocialPass et des risques liés à son utilisation sous l'aspect de la protection des données. C'est pourquoi le 31 mai 2021, jour de la réouverture des espaces intérieurs des restaurants, il a publié un communiqué de presse présentant les aspects essentiels de l'établissement des faits et les constatations établies à cette date, y compris les principales recommandations,

L'établissement des faits concernant l'application SocialPass a été nécessaire et utile. Il a permis au Préposé de se prononcer sur la délimitation entre les compétences de surveillance fédérales et cantonales ainsi que sur d'autres questions relevant de la protection des données dont certaines, en raison de leur importance fondamentale, ont pu se poser pour d'autres applications utilisées par des particuliers et des autorités pour le traçage des contacts.

MESVACCINS.CH

Enquête sur le carnet de vaccination électronique

En mars 2021, une enquête menée par le magazine en ligne Republik.ch a révélé de graves lacunes en matière de protection des données au sujet de la plateforme mesvaccins.ch. Le Préposé a ouvert une procédure formelle contre l'exploitante de la plateforme juste avant la publication de ces critiques. Les lacunes constatées ont rendu impossible la poursuite de l'exploitation de la plateforme et la fondation responsable, partiellement financée par l'OFSP, a finalement déposé le bilan. Le Préposé a coopéré avec l'OFSP dans le but de permettre aux personnes concernées de récupérer leurs données.

Dans son enquête menée au printemps 2021, le magazine en ligne Republik.ch a révélé que la plateforme mesvaccins.ch présentait de graves lacunes en matière de protection des données et de sécurité. La fondation « mesvaccins », responsable de l'exploitation, était financée en partie par l'Office fédéral de la santé publique (OFSP), lequel office faisait la promotion de ce « carnet de vaccination électronique » sur son site Internet et dans des prospectus.

Après avoir vérifié sommairement la plausibilité des reproches formulés, le Préposé a ouvert, juste avant la publication de l'article en question, une procédure d'établissement des faits concernant cette plateforme sur laquelle les utilisateurs inscrivaient leurs données de vaccination. Un audit effectué alors par la fondation a montré qu'il était difficile de remédier aux lacunes révélées par le magazine en ligne, ce qui a conduit la fondation à retirer temporairement la plateforme du réseau.

Fin juillet 2021, le Préposé a remis son rapport final à la fondation. Il y formulait trois recommandations portant en particulier sur une éventuelle atteinte à l'intégrité des données et sur leur sort en cas d'arrêt de la plateforme. Plus spécifiquement, la fondation ne pouvait pas exclure que des accès non autorisés n'aient pas déjà eu lieu par le passé et que les données n'aient pas été modifiées à cette occasion.

La fondation a accepté les recommandations du Préposé. Peu de temps après l'achèvement de la procédure d'établissement des faits, elle a fait savoir qu'elle cesserait définitivement ses activités opérationnelles et demanderait sa prochaine liquidation. Dès lors, elle n'a plus traité les demandes d'information et de suppression émanant des utilisateurs. Nombreux ont donc été les particuliers concernés qui se sont ensuite adressés au Préposé.

En outre, désireux de permettre à ceux-ci d'accéder à leurs données malgré la suspension de la plateforme et la menace de liquidation avancée par l'exploitant, le Préposé a conseillé l'OFSP au cours de plusieurs séances, ceci dans le cadre de son projet « Récupération des données », et précisé à cette occasion les exigences en matière de protection des données pour le renvoi des données de vaccination aux utilisateurs. Compte tenu des possibilités financières limitées et des lacunes constatées dans le cadre de la procédure d'établissement des faits, il est apparu clairement que certains compromis devaient être acceptés, du point de vue de la protection des données, dans le but de parvenir à une solution pragmatique et réalisable en temps utile.

En novembre 2021, sans annonce préalable, la fondation a commencé à renvoyer aux utilisateurs leurs données de vaccination non cryptées par courriel. Contrairement aux déclarations faites publiquement par la fondation, cette procédure n'a pas été convenue avec le Préposé. Elle était même en contradiction avec les recommandations émises par le Préposé dans son rapport final du 31 août 2021 ainsi qu'avec les exigences posées à l'OFSP pour un envoi conforme à la protection des données. Après intervention du Préposé, la fondation a de nouveau interrompu l'envoi des données. Elle a été ensuite déclarée en faillite. Le Préposé examine la possibilité de déposer une plainte pénale. Les clarifications nécessaires à cet effet étaient encore en cours à la fin de l'année sous revue.

Le Préposé est intervenu auprès de l'OFSP pour que celui-ci assume ses responsabilités malgré la procédure de faillite en cours et continue à œuvrer en faveur d'une solution conforme à la protection des données, afin que les utilisateurs puissent accéder à leurs données de vaccination de la manière la plus conforme possible à la protection des données.

DOSSIER PATIENT

Consultation, conservation et effacement des données des patients

Le traitement des dossiers médicaux est un thème récurrent dans les activités de conseil du Préposé, en particulier la question de savoir si et quand les patients peuvent demander à consulter ou à supprimer les données de leur dossier médical, et combien de temps les médecins doivent – et peuvent – les conserver. De plus, la modification du droit de la prescription a récemment eu des répercussions sur la conservation des dossiers médicaux.

Au cours de l'année écoulée, le Préposé a régulièrement reçu des demandes de la part de particuliers témoignant d'un grand intérêt et de nombreuses incertitudes quant à la gestion des dossiers médicaux. Le dossier médical comprend les notes et documents rassemblés par le médecin dans le cadre d'un traitement, par exemple rapports, radiographies, résultats de laboratoire et correspondance avec d'autres prestataires médicaux. Les patientes et les patients peuvent consulter leur dossier médical en vertu du droit d'accès à la protection des données. Dans la pratique, ce droit est couramment exercé.

Cependant, le droit à l'effacement de ses propres données, également prévu par la LPD, entre en conflit avec les exigences en matière de documentation imposées aux professionnels de la santé par les lois cantonales sur la santé. Ainsi, en règle générale, un médecin ne peut pas accéder à la demande d'effacement de toutes les données ou de remise de tous les documents originaux au patient car il violerait alors ses obligations légales de conservation.

En effet, la loi sur la protection des données ne donne qu'une réponse indirecte à la question de savoir combien de temps un médecin doit et peut conserver les dossiers médicaux de sa patientèle. En vertu du principe de proportionnalité, un professionnel de santé peut conserver les dossiers des patients aussi longtemps que ces documents sont encore nécessaires. Après la fin d'un traitement, ce temps de conservation peut être rallongé, par exemple à des fins de preuve jusqu'à ce que le délai de prescription pour faire valoir d'éventuelles prétentions découlant du traitement concerné soit écoulé, ou jusqu'à ce qu'il soit prévisible qu'une procédure judiciaire sera engagée. De ce fait, les délais de prescription généraux du code des obligations sont habituellement appliqués à titre de règle de base.

Ces dispositions ont été modifiées le 1er janvier 2020 : le délai de prescription pour les dommages corporels est passé de 10 à 20 ans. Certaines lois cantonales sur la santé régissant les devoirs de documentation des médecins ont déjà été adaptées en conséquence et prévoient désormais également une obligation de conservation plus longue, ce qui se répercute sur la durée de conservation des dossiers patients. La durée de conservation des documents peut être donc considérée comme étant de 20 ans.

En cas de traitement dans des hôpitaux avec mandat de prestations cantonal, c'est en général le droit cantonal qui s'applique, ainsi que les obligations et délais de conservation en vigueur.

Le dossier électronique du patient selon la LDEP

Même si les dossiers médicaux sont de plus en plus gérés sous forme numérique, ils ne constituent en général pas (encore) des dossiers électroniques de patients (DEP) au sens de la loi fédérale sur le dossier électronique du patient (LDEP). L'introduction de cette forme de documentation centrée sur le patient avance avec beaucoup de lenteur, en partie du fait de la pandémie. Toutefois, au cours de l'année sous revue, d'autres communautés de référence ont été certifiées ; les prestataires – médecins, thérapeutes, hôpitaux – peuvent s'y affilier pour pouvoir proposer un dossier électronique à leurs patients. Les premiers dossiers ont été ouverts en mai 2021.

En parallèle à l'introduction du DEP, plusieurs voix se sont élevées – notamment dans le monde politique – pour en demander des modifications afin de promouvoir sa diffusion. Le Préposé suit les interventions et les développements sur le sujet et entretient des contacts réguliers avec l'OFSP, les cantons et autres acteurs.

SÉCURITÉ DES REGISTRES

Vulnérabilité des registres du don d'organes et des implants mammaires

La protection des données dans le cadre de l'exploitation de registres dans le domaine de la santé ne semble pas suffisamment considérée. Sur le premier trimestre 2022, le PFPDT est intervenu dans plusieurs cas problématiques qui ont été notamment relayés par les médias.

Depuis le début de l'année 2022, les médias ont notamment attiré l'attention sur deux registres, présentant des lacunes importantes du point de vue de la protection des données.

Dans le premier cas, concernant le registre national du don d'organes mis en place et géré par la fondation Swisstransplant, le problème portait essentiellement sur l'exactitude des données saisies. Il était en effet possible d'inscrire au registre – et donc d'inscrire « sa » déclaration pour ou contre le don d'organes – une personne tierce, sans que celle-ci n'ait connaissance de la démarche. Après avoir vérifié la plausibilité des faits portés à sa connaissance et pris les premières mesures pour limiter les dégâts, le PFPDT a ouvert une procédure d'établissement des faits (art. 29 LPD), à l'occasion de laquelle les processus d'identification seront notamment évalués et améliorés.

Ce cas présente aussi une composante politique, eu égard aux votations du 15 mai 2022. Le peuple est invité à se prononcer sur un changement de système en matière de don d'organes ; aujourd'hui, il faut un consentement explicite pour qu'un prélèvement puisse intervenir. Avec la modification proposée, ce serait l'inverse : à défaut d'opposition, le prélèvement serait autorisé (consentement présumé). Cette modification s'accompagnerait de la création d'un nouveau registre, où l'on pourrait consigner sa décision en la matière ; à noter qu'il est question d'un registre différent de celui ici en cause, même si sa finalité est similaire.

Le second cas concernait le registre des implants mammaires géré par Swiss Plastic Surgery. Il présentait des lacunes informatiques et des erreurs de conception, permettant à des personnes non-autorisées une consultation large – et relativement aisée – des données des patientes. Dans ce cas également, le Préposé a vérifié la plausibilité des faits dénoncés et engagé des mesures pour réduire les dommages. La suite de la procédure fait actuellement l'objet d'une évaluation par le PFPDT.

D'une manière générale, ces deux cas récents et l'affaire de la fondation mesvaccins.ch (voir article plus haut) démontrent que la sécurité des registres gérés par des associations privées et des fondations, qui traitent parfois aussi des données personnelles sur mandat des autorités sanitaires, est souvent négligée. Le PFPDT insiste sur le fait que la création d'un registre implique de la part de ses exploitants d'avoir pleinement conscience de leur responsabilité, tant en regard de la sécurité des données que de leur exactitude. En conséquence, il est indispensable de disposer d'un concept complet de gestion des données, depuis leur collecte jusqu'à leur destruction. Cela suppose une organisation IT, mais aussi une organisation du personnel et une gestion des accès adéquates. Sans oublier l'information des personnes dont les données sont collectées : à défaut de motifs justificatifs, dont le responsable du registre pourrait se prévaloir, celles-ci doivent pleinement connaître l'utilisation envisagée de leurs données avant d'y consentir.

CYBERATTAQUES

Dossiers de patients publiés sur le darknet

En mars 2022, des médias romands ont rapporté qu'une grande quantité de données médicales avait été publiée sur le darknet. Le PFPDT a exigé que les cabinets médicaux concernés informent correctement leur patientèle sur cet incident. Les cabinets romands visés avaient déjà pris les premières mesures pour pallier aux déficits en matière de protection et de sécurité des données.

Ce piratage est un nouveau signal d'alerte montrant que les données médicales sensibles ne font souvent pas l'objet d'une protection suffisante en Suisse. Le PFPDT espère que les médecins et les représentants de la branche reconnaîtront l'urgence d'agir en ce domaine.

1.5 Secteur du travail

PERSONNEL DE LA CONFÉDÉRATION

Clarifications auprès de l'Office fédéral de la statistique concernant la conservation des dossiers physiques du personnel

Le PFPDT a entrepris des clarifications auprès de l'Office fédéral de la statistique (OFS) au sujet de la gestion des dossiers physiques des anciens collaborateurs. Il s'est avéré qu'il y avait lieu d'agir. L'OFS l'a reconnu et a soumis au Préposé une proposition visant à rétablir une situation conforme au droit.

Le droit du personnel de la Confédération prévoit que les dossiers du personnel sont conservés pendant 10 ans après la fin des rapports de travail. Passé ce délai, les dossiers sont proposés aux Archives fédérales, qui détruisent ensuite les données sans valeur archivistique. Suite à la demande d'un particulier, le Préposé a appris que l'OFS conservait probablement un grand nombre de dossiers du personnel au-delà des délais autorisés par la loi. Le Préposé a donc entrepris des premiers éclaircissements auprès de l'OFS.

Il en est ressorti que la conservation des dossiers physiques des anciens collaborateurs ne respectait pas les dispositions légales. Pendant une longue période, les dossiers des anciens collaborateurs n'ont pas été détruits après 10 ans. L'OFS a reconnu la nécessité d'agir et a, sur la demande du Préposé, présenté un plan de mise en œuvre et un calendrier afin de rétablir une situation conforme au droit. Les travaux nécessaires devraient prendre fin à l'été 2022. Dans ce contexte, le Préposé a pu renoncer à une procédure de surveillance formelle au sens de l'art. 27 LPD.

1.6 Assurances

SURVEILLANCE DANS LE DOMAINE DE L'ASSURANCE-MALADIE

Clarification des rôles et compétences entre l'OFSP et le PFPDT

Le PFPDT et l'Office fédéral de la santé publique ont entrepris des démarches de clarification des rôles et de renforcement de leurs échanges suite à un audit du Contrôle fédéral des finances relevant l'existence de chevauchement des compétences au niveau de la mise en œuvre de la surveillance des assureurs-maladie.

Dans le cadre de leurs activités, les assureurs-maladie doivent respecter les dispositions relevant des assurances sociales et de la protection des données. Ils sont ainsi soumis à la surveillance tant de l'Office fédéral de la santé publique (OFSP) que de celle du PFPDT. Dans un rapport d'audit du 21 mai 2021 mené auprès de l'OFSP concernant la surveillance dans le domaine des assurances, le Contrôle fédéral des finances (CDF) a relevé qu'une clarification des rôles et la mise en place d'échanges et de coordination s'imposaient entre le PFPDT et l'OFSP (Audit CDF-20424).

Définir les rôles et les règles de communication

Dans son appréciation, le CDF a précisé que l'efficacité de la surveillance des assureurs-maladie entre le PFPDT et l'OFSP doit être maintenue voire même renforcée. La surveillance auprès des assureurs-maladie doit tirer profit de l'expérience et de la proximité de l'OFSP via ses interventions sur site et des compétences légales renforcées du PFPDT avec la révision de la loi fédérale sur la protection des données. Le CDF a ainsi recommandé à l'OFSP, en collaboration avec le PFPDT, de définir les rôles et les règles de communication des cas de non-conformité entre les assureurs-maladie et les organes de surveillance. Il ressort également du rapport du CDF que l'Office fédéral de la justice (OFJ) a précisé les compétences du PFPDT et de l'OFSP dans la mise en œuvre des exigences légales de protection des données en concluant à une compétence prépondérante du PFPDT. L'OFSP a dès lors décidé d'adapter en conséquence sa circulaire no 7.1 du 17 décembre 2015 « Assureurs-maladie : Organisation et processus conformes à la protection des données ».

Clarifier les responsabilités

Dans sa prise de position sur le rapport d'audit du CDF, le PFPDT s'est déclaré favorable à une coordination des activités de surveillance de l'OFSP et du PFPDT dans le domaine de l'assurance-maladie compte tenu du chevauchement des compétences ainsi qu'à la clarification des rôles et des responsabilités. Le PFPDT a toutefois rappelé que son indépendance vis-à-vis des efforts de coordination dans le domaine de l'assurance-maladie devait rester garantie. Il continuera en particulier à assumer sa fonction de surveillance vis-à-vis de l'OFSP.

Renforcer les échanges

À la lumière des considérations du CDF développées dans son rapport d'audit, le PFPDT a collaboré aux travaux de révision de la circulaire no 7.1 de l'OFSP. Il a émis différentes propositions de compléments, en particulier concernant la coordination lors de chevauchement de compétences. Il a ainsi été précisé dans le projet de circulaire que l'OFSP et le PFPDT, dans le respect de leurs compétences légales respectives, s'échangent de manière régulière, ainsi que de manière ad hoc selon les besoins de coordination de cas d'espèce et d'efficacité de leurs tâches de surveillance, en particulier par leur coopération et partage de leurs connaissances matérielles dans leurs domaines respectifs de l'assurance-maladie et de la protection des données. Il a également été ajouté à l'attention des assureurs que la suppression dans la nouvelle circulaire de certains chapitres ne signifiait pas pour autant que les assureurs étaient dispensés de leurs obligations légales. Pour ce qui concerne la compétence d'examen de la conformité de protection des données du PFPDT ainsi que l'examen matériel des règlements, il a été précisé que le PFPDT agira en tant qu'autorité de surveillance indépendante et selon ses ressources et priorités. La nouvelle version de cette circulaire no 7.1 a été transmise par l'OFSP à tous les assureurs-maladie en décembre 2021 et est entrée en vigueur le 1er janvier 2022.

En marge des discussions relatives à la révision de cette circulaire, l'OFSP et le PFPDT ont convenu de la désignation de personnes de contact ainsi que de la mise en place d'une réunion d'échange annuelle et de séances ad hoc allant dans le sens des considérations du CDF de renforcer l'efficacité de leurs tâches de surveillance.

1.7 Transports

CARPOSTAL ET CFF

Failles de sécurité dans les portails clients

Faute de précautions techniques sur leurs systèmes informatiques, CarPostal et les CFF ont subi pendant l'année sous revue des fuites de données sur leurs portails « ticketcontrol.ch » et « Nova ». Le PFPDT a vérifié auprès des conseillers à la protection des données des deux entreprises que le nécessaire avait été fait pour pallier ces faiblesses et pour informer les clients.

Dans le cadre d'une recherche, un groupe de journalistes s'est aperçu qu'il était facile de consulter et de copier des données sur le portail clients « ticketcontrol.ch ». Ils en ont informé CarPostal SA, l'exploitant du portail, et le PFPDT qui a immédiatement exigé des explications de la part de l'entreprise responsable. CarPostal a réagi rapidement, confirmant le problème. L'analyse des protocoles d'accès a permis de retracer l'attaque et de l'attribuer à des agresseurs spécifiques. Dans le cadre de l'enquête, CarPostal a pu démontrer au Préposé que la faille avait été corrigée très rapidement après avoir été découverte, et que les données obtenues lors de la recherche ont été détruites. Le PFPDT a aussi eu connaissance d'une faille de sécurité sur la plateforme centrale de distribution « Nova » qu'exploitent les CFF sur mandat d'Alliance SwissPass. Un spécialiste de l'investigation informatique a révélé avoir réussi à consulter en un court laps de temps jusqu'à un million de lots de données portant sur des billets et des abonnements. Les CFF ont confirmé cette fuite au Préposé et corrigé la faille immédiatement. Ils lui ont aussi annoncé que les autres entreprises de transport concernées avaient pris les mesures d'urgence nécessaires et que les clients n'avaient subi aucun dommage. L'expert informatique a effacé les données qu'il avait téléchargées.

Dans les deux cas, les conseillers en protection des données des entreprises ont assuré que les mesures prises avaient permis de supprimer tout risque systémique démesuré sur les plateformes en question et que les personnes concernées avaient étés informées de manière appropriée. Pour le PFPDT, l'augmentation du nombre d'attaques ciblant des systèmes informatiques est la preuve que les exploitants doivent consacrer plus de ressources à la sécurité de l'exploitation. Les systèmes présentant un risque accru pour les personnes concernées devraient en outre faire régulièrement l'objet d'audits externes.

DONNÉES PNR

Consultation des offices relative à la nouvelle loi sur les données de passagers aériens

Le DFJP a élaboré un projet législatif visant à pouvoir utiliser en Suisse, aux fins de lutte contre le terrorisme et la criminalité, les données de passagers recueillies par les compagnies aériennes. Le Préposé a pris position à ce sujet dans le cadre de la consultation des offices.

En réservant un vol, les futurs passagers communiquent de nombreuses informations aux compagnies aériennes ou aux agences de voyage. Ces informations doivent pouvoir être utilisées par les autorités de police et de sécurité pour prévenir le terrorisme et la grande criminalité. De nombreux pays européens ont déjà mis en place des services ad hoc (les Unités Informations Passagers UIP) recueillant, enregistrant et traitant les données des passagers aériens. Par exemple, ces données doivent pouvoir être comparées avec les bases de données des organes de poursuite pénale afin que les personnes susceptibles d'être impliquées dans un acte relevant du terrorisme ou de la grande criminalité soient identifiées.

Selon la décision du Conseil fédéral du 12 février 2020, la Suisse aussi devrait pouvoir utiliser les données des dossiers passagers (données PNR Passenger Name Record). En juin 2021, le DFJP a donc élaboré, en collaboration avec le DETEC, un projet de consultation sur une loi fédérale relative à la collecte et à l'utilisation par la Suisse des données PNR ainsi qu'à leur transfert vers des États dont la protection

et le traitement des données correspondent aux normes de la directive européenne 2016/681 du 27 avril 2016 relative à l'utilisation des données des dossiers passagers 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 (directive PNR de l'UE).

Une liste des infractions requise

Dans sa prise de position sur un premier projet, le Préposé a demandé que les principes de la protection des données soient respectés dans chacune des dispositions. Il a notamment requis que la marge de manœuvre préventive des UIP soit clairement définie et que le Service de renseignement de la Confédération (SRC) n'ait qu'un accès limité au système d'information PNR. De plus, une liste exhaustive des infractions doit indiquer dans quel but les données peuvent être collectées. Le Préposé a également souligné que la proportionnalité doit être respectée. Il conviendrait par exemple de justifier pourquoi la durée de conservation de cinq ans est nécessaire pour atteindre le but poursuivi (cf. 28e rapport d'activités, ch. 1.8).

Une nouvelle consultation des offices est prévue pour janvier 2022.

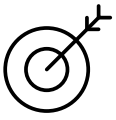
APPLICATIONS DE STATIONNEMENT

Parcomètres numériques avec saisie du numéro de plaque d'immatriculation

Au cours de l'année sous revue, le Préposé a reçu un certain nombre de questions au sujet des parcomètres numériques qui exigent la saisie du numéro de plaque d'immatriculation. Dans ce contexte, il s'est prononcé sur les parkings gérés par des sociétés privées.

Durant l'année sous revue, le Préposé a noté une augmentation du nombre de questions de particuliers en lien avec les parcomètres numériques. Ces citoyens s'inquiétaient de savoir s'il est correct, sur le plan de la protection des données, d'être obligé de saisir son numéro d'immatriculation pour s'enregistrer.

Les numéros de plaque d'immatriculation peuvent être saisis et traités à



des fins d'enregistrement dans les parcomètres numériques. Toutefois, ces données ne peuvent être conservées que pendant le temps strictement nécessaire pour atteindre l'objectif visé. Conformément au principe de transparence établi par la législation sur la protection des données, le responsable du traitement des données doit informer les personnes concernées, par des moyens appropriés, de la finalité de la collecte des données, ainsi que du traitement et de la durée de conservation qui y sont liés, si ceux-ci ne ressortent pas déjà clairement des circonstances.

Nous avons signalé aux personnes nous ayant contactés que, conformément à l'art. 8 LPD (RS 235.1), elles peuvent demander au maître du fichier si des données les concernant sont traitées, lesquelles et dans quel but. Des modèles de lettres à ce sujet sont disponibles sur le site Internet du Préposé.

CONDUITE AUTOMATISÉE

Consultation des offices sur la révision partielle de la loi sur la circulation routière

Plusieurs modifications ont été apportées à la loi sur la circulation routière durant l'exercice écoulé. Elles ont permis entre autres de réglementer la conduite automatisée en Suisse. Le Préposé a accompagné cette révision et s'est prononcé dans le cadre de la consultation des offices. Il a demandé que le rapport explicatif relatif à la loi clarifie les questions de proportionnalité, notamment en ce qui concerne la durée de conservation des données et leur effacement.

La modification de la loi sur la circulation routière (LCR), placée sous la direction de l'Office fédéral des routes (OFROU), a pour but d'ouvrir la voie à la conduite automatisée en Suisse. Le Conseil fédéral pourra désormais définir dans quelle mesure les conducteurs seront déchargés de leurs obligations et dans quel cadre les véhicules sans conducteur équipés d'un système d'automatisation seront autorisés. Selon le projet de révision, ce type de véhicules pourra circuler sur des tronçons prédéfinis tout en étant surveillés.

Les véhicules équipés d'un système d'automatisation doivent être dotés d'un enregistreur de mode de conduite qui ne doit pas pouvoir être désactivé et qui conserve certains événements en rapport avec le système d'automatisation. Par exemple, le moment où le conducteur passe en mode de conduite automatique (ou le quitte), le moment où le système demande au conducteur de reprendre le contrôle du véhicule

ou encore l'apparition d'éventuelles défaillances techniques sont enregistrés automatiquement.

Du point de vue du Préposé, les informations enregistrées par l'enregistreur de mode de conduite peuvent être facilement reliées à des données personnelles telles que celles du détenteur du véhicule. C'est pourquoi nous avons approuvé le fait que l'horodatage soit enregistré, et non les données de localisation. Nous avons en outre insisté pour qu'il ressorte clairement de la LCR et de ses commentaires explicatifs qui peut avoir accès aux données de l'enregistreur de mode de conduite et à quelles fins clairement définies, et de préciser si et quand ces données peuvent être analysées en fonction d'une personne déterminée. Cela devrait éviter qu'elles soient utilisées dans des buts quelconques.

En outre, le Préposé s'est penché sur la question de la proportionnalité, notamment en ce qui concerne le délai d'effacement qui s'étend jusqu'à ce que la mémoire du système soit pleine. Le délai d'effacement des données peut donc varier en fonction de l'utilisation du véhicule. Le Préposé a requis que les notes explicatives à ce sujet soient complétées. Il a également demandé que l'effacement des données après la mise hors circulation du véhicule soit précisé dans les commentaires explicatifs.

L'OFROU a intégré les suggestions du Préposé au projet de loi. Le 17 novembre 2021, le Conseil fédéral a adopté le message concernant la révision de la loi sur la circulation routière et l'a soumis au Parlement.

DONNÉES SUR LA MOBILITÉ

L'échange de données sur la mobilité nécessite une base légale

La Confédération veut encourager une mobilité efficace et intermodale, notamment en favorisant la combinaison de moyens de transport différents. Pour ce faire, les services et les données relatifs aux différentes offres de mobilité doivent être rendus accessibles aux utilisateurs concernés et mis à leur disposition. Le PFPDT a pris position concernant le projet de loi à ce sujet dans le cadre de la consultation des offices.

La loi fédérale concernant l'infrastructure de données sur la mobilité (LIDMo) permettra de réaliser progressivement une infrastructure nationale de données pour la mobilité (NADIM) en vue de faciliter l'échange de données sur la mobilité. La NADIM sera exploitée par le futur centre des données sur la mobilité (CDM). Des entreprises privées, comme les développeurs d'application et les exploitants de plateformes, pourront ainsi proposer à leur clientèle des offres en réseau.

Les données sur la mobilité au sens du projet de loi sont en premier lieu des données techniques telles que les informations sur les systèmes de transport, les horaires ou les tarifs. En fonction des offres, les données personnelles des clients sont nécessaires pour la réservation et le paiement. Selon les circonstances, des profils de déplacement ou – en lien avec des offres de voyage pour des personnes à mobilité réduite – des données sensibles pourront également être traités par le CDM. D'après l'OFT, le projet doit toutefois encore évoluer pour que l'on dispose de plus de détails à ce sujet.

En premier lieu, le PFPDT a demandé la création de la base légale nécessaire pour les catégories de données que le CDM traitera. Il a également signalé la nécessité d'examiner dans les meilleurs délais la possibilité de procéder à une analyse d'impact relative à la protection des données personnelles, comme le prévoit l'art. 22 nLPD. Une telle analyse permet de déterminer quels sont, pour la sphère privée et l'autodétermination informationnelle des personnes concernées,

les risques liés au traitement des données personnelles sur la base de leur finalité, de leur contenu ou de leur nature, mais aussi de l'étendue ou de la durée du traitement.

Selon l'OFT, le traitement concret des données et d'autres détails importants relatifs à la mise en œuvre ne seront connus que dans une phase ultérieure du projet. En conséquence, le PFPDT ne pourra se prononcer de manière définitive sur l'ensemble du projet qu'une fois que les informations pertinentes seront disponibles.


Reihe
Row
5

1.8 International

Au cours de l'année écoulée, la coopération internationale a de nouveau été marquée par la crise du COVID-19. En raison de la pandémie, la plupart des conférences et réunions internationales ont eu lieu en ligne. La 43e Conférence internationale des commissaires à la protection des données et de la vie privée, prévue au Mexique en octobre 2021, aurait dû se tenir en mode hybride, mais elle n'a finalement pu avoir lieu que sous forme virtuelle. Quant à la Conférence européenne des commissaires à la protection des données et de la vie privée, qui a lieu chaque année, elle a, dans un premier temps, été reportée à une autre date en 2021, avant d'être annulée. Dans le cadre de l'OCDE, le PFPDT a également participé à diverses réunions virtuelles, par exemple sur les thèmes de la « Data Governance and Privacy Challenges in the Fight against COVID-19 » et de la « Data Localisation and Trusted Government Access to Data ».

Lorsque les rencontres internationales ont lieu uniquement sous forme de vidéoconférences, il devient plus difficile de mener des discussions informelles et de nouer des contacts directs. Par contre, grâce aux économies de coûts et de temps , un nombre plus important que d'ordinaire d'autorités de protection des données et de personnes par autorité ont pu suivre les vidéoconférences.

L'année sous revue a montré une nouvelle fois l'importance de la dimension internationale de la protection des données. En raison des activités déployées à l'échelle internationale par de nombreuses entreprises, plusieurs questions délicates se posent concernant la protection des données, notamment en lien avec le flux transfrontière de données personnelles (communication directe de données ou stockage dans des clouds et sur des serveurs à l'étranger).

Le Préposé reste 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

Protection de la vie privée des enfants dans l'environnement numérique et lignes directrices relatives au profilage et aux campagnes politiques

Lors de ses cinq réunions, le Comité consultatif de la Convention 108 s'est penché notamment sur l'élaboration de deux documents adoptés par le Comité des Ministres en 2021. Il s'agissait d'une part de la Déclaration sur la protection de la vie privée des enfants dans l'environnement numérique et d'autre part de la modification de la Recommandation du Comité des ministres concernant le profilage. Le Comité a également adopté des lignes directrices relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par et pour les campagnes politiques.

En 2021, tout comme au cours de l'exercice précédent, les réunions du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108) ont été organisées par visioconférence en raison de la pandémie. De même, les réunions de son Bureau, au sein duquel siège une représentante du Préposé, ont eu lieu uniquement en mode virtuel. Le Comité s'est penché sur des questions de protection des données

relatives à différents thèmes importants. Dans le même temps, il a adopté son programme de travail pour la période 2022–2025. Le Comité a pris position entre autres sur le projet de deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest). Il a notamment souligné l'importance de trouver un régime de protection des données garantissant une poursuite pénale efficace tout en promouvant la protection des personnes concernées par le traitement des données.

Le Comité a participé aux travaux préparatoires de deux documents qui ont été adoptés par le Comité des ministres en 2021. Il s'agissait en premier lieu de la Déclaration du Comité des ministres sur la protection du droit des enfants à la vie privée dans l'environnement numérique. Cette déclaration a été élaborée par le Comité directeur des droits de l'enfant du Conseil de l'Europe, en collaboration avec le Comité consultatif. Les États membres y sont invités à renforcer la protection de la vie privée et des données personnelles des enfants, en particulier de leurs données relatives à la santé et de celles collectées dans le cadre éducatif, ceci notamment dans le contexte de la pandémie de COVID-19 afin de minimiser les effets négatifs potentiels de l'identification publique d'un enfant comme porteur du coronavirus.

L'autre document concernait la Recommandation sur la protection des personnes à l'égard du traitement des données personnelles dans le cadre du profilage. Cette recommandation prévoit que le respect des libertés et des droits fondamentaux dans le secteur public comme dans le secteur privé soit garanti dans tous les traitements de profilage. Elle remplace une déclaration antérieure datant de 2010 et tient compte de l'évolution technologique de ces dernières années. Son texte est aligné sur celui de la convention modernisée pour la protection des données personnelles, connue sous le nom de Convention 108+.

Dans sa déclaration intitulée « Vaccination, attestations COVID-19 et protection des données », le Comité a rappelé l'importance de trouver un équilibre entre la protection des droits et des libertés fondamentales et les enjeux de santé publique liés à la pandémie.

Le Comité a également adopté des lignes directrices sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par et pour les campagnes politiques. Celles-ci régissent l'application de la Convention 108+ aux campagnes politiques, compte tenu du nombre croissant de stratégies de campagnes numériques passant par les médias sociaux.

En outre, le Comité a décidé de réviser le contrat type du Conseil de l'Europe visant à assurer une protection appropriée dans le contexte des flux transfrontières de données. Les travaux, pour lesquels la Suisse est le rapporteur, en sont encore à leur début.

ATELIER EUROPÉEN DE TRAITEMENT DES DOSSIERS

Améliorer la collaboration entre les autorités de protection des données

Comme chaque année, le Préposé a participé à l'Atelier européen de traitement des dossiers (European Case Handling Workshop), organisé en 2021 par les autorités de protection des données de Gibraltar.
En raison de la pandémie, cette rencontre a eu lieu virtuellement les 16 et 17 novembre 2021. Plus de 120 participants provenant de 30 autorités chargées de la protection des données y ont participé. Ils ont abordé des questions concernant la notification des violations de la protection des données, le traitement interne des plaintes et l'application des mesures. Les répercussions de l'arrêt de la Cour de justice de l'UE, communément appelé « arrêt Schrems II », ont également été discutées.

Cet atelier annuel vise à favoriser la coopération entre autorités et surtout à en améliorer l'efficacité. Il est d'une grande utilité pratique pour les autorités de contrôle, surtout pour les autorités de petite taille, et leur offre une plateforme permettant d'échanger expériences et connaissances. Dans la perspective de l'entrée en vigueur de la nouvelle loi sur la protection des données (cf. Accent I) et de l'assistance administrative que celle-ci prévoit, ces échanges et le développement des compétences deviendront essentiels aux yeux du Préposé, qui s'est donc proposé d'accueillir l'Atelier européen de traitement des dossiers en Suisse, à l'automne 2023.

ASSEMBLÉE MONDIALE

Réunion en ligne de plus de 90 membres et observateurs

La 43e Assemblée mondiale pour la protection de la vie privée (AMVP), antérieurement nommée la Conférence internationale des commissaires à la protection des données et de la vie privée, s'est tenue du 18 au 21 octobre 2021, pour la deuxième fois en ligne en raison de la crise sanitaire.

La conférence virtuelle a été organisée par l'Institut national pour la transparence, l'accès à l'information et la protection des données personnelles (INAI), au Mexique, et a réuni plus de 90 membres et observateurs pour examiner les principaux défis en matière de protection des données. Elle avait pour thème « La protection de la vie privée et des données : une approche axée sur l'être humain ».

Un droit fondamental

La 43e session à huis clos de l'Assemblée mondiale de la protection de la vie privée (AMVP) a été ouverte par Elizabeth Denham, commissaire à l'information du Royaume-Uni, qui a salué le travail de la communauté de la protection de la vie privée pendant la pandémie, appelant à ce que l'Assemblée continue d'avoir un tel impact.

« L'objectif de cette conférence est de faire en sorte que l'on passe de la protection des données personnelles à la protection de la vie privée des personnes en tant que droit fondamental », a déclaré l'hôte de la conférence, Blanca Lilia Ibarra Cadena, présidente-commissaire de l'Institut national pour la transparence, l'accès à l'information et la protection des données personnelles du Mexique.

Durant la session fermée, des résolutions ont été discutées puis approuvées lors de la conférence, donnant un point de vue partagé sur une gamme de sujets d'actualité importants :

- le partage de données pour le bien public ;
- les droits numériques des enfants ;
- l'accès du gouvernement aux données ;
- l'avenir de l'AMVP ;
- la coopération internationale en matière d'application de la loi ;
- et les bacs à sable réglementaires.

Nouveau plan stratégique

Les participants à la conférence ont adopté un nouveau plan stratégique sur deux ans pour l'AMVP, lequel vise à créer un environnement permettant aux autorités de protection des données et de la vie privée de remplir concrètement leur mandat, à savoir assurer des normes élevées de protection des données à l'échelle mondiale ainsi que promouvoir et faciliter une coopération efficace en matière de réglementation.

L'AMVP a également annoncé les lauréats des prix mondiaux de la vie privée et des données de 2021. Ces prix soulignent les réalisations des responsables mondiaux de la protection de la vie privée et mettent en lumière les enquêtes notables, les bonnes pratiques et les initiatives de sensibilisation du public.

AMPV – GROUPE DE TRAVAIL

Protection des données dans l'aide internationale au développement

Un an après son instauration, le Groupe de travail sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide internationale humanitaire et la gestion de crise (GT AID) dresse un premier bilan de ses activités.

Le Groupe de travail consacré au rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide internationale humanitaire et la gestion de crise a été mis en place suite à une résolution de l'Assemblé mondiale pour la protection des de la vie privée (AMVP) lors de sa 42e conférence annuelle en 2021. Le GT AID, présidé par le PFPDT, compte plus de 20 membres et sa composition reflète la diversité géographique de l'AMVP.

Au cours de sa première année d'existence, le GT AID s'est concentré sur l'élaboration d'un plan de travail conforme aux priorités stratégiques de l'AMVP. Celles-ci concernent en particulier :

- la progression de la protection de la vie privée à l'échelle mondiale ;
- 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, y compris au moyen d'accords avec des organismes ayant un rôle d'observateur ;
- les droits de la personne et la protection sociale ainsi que les droits démocratiques.

Objectifs généraux

Conformément aux priorités visées dans la résolution, les membres du GT AID se sont fixés les objectifs généraux suivants :

- répondre à la demande de coopération des acteurs pertinents (p. ex. agences de développement, acteurs humanitaires) pour développer des lignes directrices et échanger les meilleures pratiques en matière de protection des données personnelles et de la vie privée. Ceci en tenant compte des spécificités de l'aide internationale au développement et de l'action humanitaire internationale ainsi que du besoin de faciliter ces activités ;
- développer une stratégie de plaidoyer et de mobilisation auprès des acteurs pertinents.

Afin d'atteindre ces deux objectifs, le GT AID a décidé de mettre en place des activités permettant :

- d'affiner la compréhension de l'aide internationale au développement, de l'aide internationale humanitaire et de la gestion de crise ;
- d'établir un contact pérenne avec les acteurs pertinents, tant au niveau bilatéral que multilatéral et ainsi maximiser la portée de la voix de l'AMVP en renforçant les relations avec les acteurs de l'aide internationale au développement ;
- en lien avec les autres groupes de travail de l'AMVP, produire des documents et outils de plaidoyer en faveur d'une meilleure prise en compte de la protection des données personnelles et de la vie privée dans les activités concernées ;
- de promouvoir et faciliter, pour les pays bénéficiaires de ces activités qui ne sont pas dotés d'un cadre de protection des données personnelles et de la vie privée, leur intégration à la communauté mondiale de la protection des données personnelles et de la vie privée.

Dans le cadre de ces activités, les membres du GT AID ont élaboré une cartographie de l'aide internationale au développement et de l'aide humanitaire internationale. Ils ont également identifié les pays bénéficiaires de ces activités qui ne sont pas dotés d'un cadre de protection des données personnelles et de la vie privée. De plus, le GT AID a rédigé un questionnaire et une lettre d'accompagnement qui lui permettra d'affiner sa compréhension du travail des acteurs concernés.

SYSTÈMES D'INFORMATION SCHENGEN

Groupes de coordination de contrôle SIS II, VIS et Eurodac

Les groupes de coordination de contrôle (GCC) du SIS et du VIS ont adopté une lettre commune concernant la proposition législative de la Commission européenne visant à adapter le mécanisme d'évaluation de Schengen.
Comme l'année précédente, les trois GCC des systèmes d'information de l'UE – SIS II, VIS (présidence assurée par le Préposé) et Eurodac – ont organisé leurs deux rencontres annuelles par visioconférence en raison de la pandémie de COVID-19. Ces réunions ont eu lieu les 16 et 17 juin 2021 et les 24 et 25 novembre 2021. Elles ont rassemblé le contrôleur européen de la protection des données (CEPD) et les autorités nationales de protection des données des États membres.

Le GCC VIS a adopté un questionnaire sur l'effacement anticipé des données : celles-ci doivent être effacées de façon anticipée dès lors que la personne concernée obtient la nationalité d'un État membre et n'a donc plus besoin d'un visa Schengen. Les autorités de protection des données des États membres sont maintenant invitées à diffuser ce questionnaire au niveau national afin de vérifier la mise en œuvre de l'effacement anticipé dans les différents États.

Au cours de leur rencontre de novembre, les GCC SIS et VIS ont rédigé et adopté une lettre commune concernant la proposition législative de la Commission européenne visant à adapter le mécanisme d'évaluation de Schengen. Cette lettre a mis l'accent sur l'importance de faire appel en premier lieu à des experts émanant des autorités de protection des données pour procéder aux évaluations Schengen en matière de protection des données. Elle précisait également que ces experts devaient être convoqués plus tôt que prévu, à savoir quatre mois à l'avance et non pas seulement onze semaines. Cette lettre a été envoyée au Conseil, à la Commission et au Parlement de l'Union européenne.

En collaboration avec l'Agence des droits fondamentaux de l'Union européenne, le GCC Eurodac a adopté un guide permettant aux autorités de mieux informer les personnes au moment de la prise de leurs empreintes digitales pour Eurodac. Ce guide a été distribué en Suisse aux autorités compétentes et publié sur différents sites Internet.

ROYAUME-UNI

Brexit – adéquation du niveau de protection des données

Du point de vue suisse, il n'y a eu aucune modification du statut d'adéquation du Royaume-Uni. Celui-ci figure toujours sur la liste des États du Préposé en tant que pays offrant un niveau de protection équivalent.

SYSTÈMES DE VIDÉOCONFÉRENCE

Les bonnes pratiques des autorités de protection des données

Depuis le début de la pandémie, les autorités et les entreprises privées ont de plus en plus misé sur les plateformes de communication vidéo. En collaboration avec les autorités de protection des données de cinq autres États, le PFPDT a demandé aux entreprises Microsoft, Google, Cisco et Zoom de présenter leurs plateformes de vidéoconférence et d'engager un dialogue ouvert.

Au cours de l'échange avec les entreprises de vidéoconférence, les autorités se sont concentrées sur les thèmes de la sécurité, du respect de la vie privée dès la conception et par défaut (Privacy by design and default), de la connaissance de son public (Know your audience) et de la transparence. Le dialogue s'est avéré bénéfique tant pour les autorités que pour les entreprises concernées. Il a débouché sur une déclaration rassemblant les bonnes pratiques, disponible sur le site Internet du PFPDT. Quelques mesures sont présentées ici. (voir encadré ci-contre).

Il est en outre important que les fournisseurs de services de vidéoconférence établissent une relation de confiance avec les utilisateurs en ne traitant les informations les concernant que de façon justifiée, aux yeux de ceux-ci, par les circonstances. Les données personnelles ne devraient ainsi être saisies que dans la mesure où elles sont nécessaires pour l'utilisation des fonctions clés du service de vidéoconférence. Les utilisateurs devraient être informés de manière totalement transparente de l'endroit où les données sont sauvegardées et des canaux par lesquels elles sont transmises. Par ailleurs, les utilisateurs devraient avoir le choix des sites par lesquels leurs données personnelles transitent et de l'endroit où elles sont stockées.

Le document publié sur le site n'est pas exhaustif, et les entreprises proposant de telles offres doivent en outre respecter les dispositions relatives à la protection des données en Suisse et les explications du PFPDT relatives à la transmission des données à l'étranger.

Sécurité

- Il est indispensable de tester régulièrement les mesures de sécurité pour s'assurer qu'elles restent fiables compte tenu de l'évolution constante des menaces.
- Les collaborateurs doivent être régulièrement formés en matière de sécurité et de protection des données.
- Audit régulier des tiers, y compris la journalisation de l'accès des sous-traitants aux données se rapportant à des personnes, et le principe du moindre privilège devrait s'appliquer lors du contrôle de l'accès.

Transparence

- Les utilisateurs doivent être informés du comment et du pourquoi leurs données sont saisies et utilisées.
- Ils doivent être clairement informés des personnes auxquelles leurs données sont communiquées et pourquoi.

Respect de la vie privée dès la conception et par défaut

- Avant l'implémentation de nouvelles solutions et fonctions de vidéoconférence, il faut procéder à une analyse d'impact sur la protection des données et garantir un échange régulier entre les équipes chargées de la protection des données, de la sécurité et du développement.
- Le principe de la minimisation des données doit être respecté.
- Les entreprises de vidéoconférence devraient veiller à ce que les paramètres de leurs services présentent par défaut le standard maximal en matière de protection des données.

Connaissance de son public

- Les entreprises de vidéoconférence doivent mettre en place des mesures robustes sur les plans de la sécurité et de la protection des données pour protéger de façon appropriée les données se rapportant à des personnes dans les environnements plus sensibles tels que la santé et la formation.
- Des instructions sur la sécurité et la protection des données taillées sur mesure pour des groupes déterminés sont nécessaires afin que la sécurité soit garantie pour tous les utilisateurs lors de vidéoconférences et que ceux-ci puissent choisir les fonctions et paramètres les plus appropriés à leurs besoins.

Cryptage de bout en bout

- Il convient de viser un cryptage de bout en bout, dans lequel la clé est établie par l'organisateur de la séance et l'accès aux données concernées n'est octroyé qu'aux participants et à l'organisateur.
- L'utilisation standard du cryptage de bout en bout dans les entretiens individuels sensibles, par exemple en télémédecine, est importante.

Transfert de données vers l'étranger

CLAUSES CONTRACTUELLES TYPES

Transfert de données personnelles vers un pays sans niveau de protection des données adéquat

Dans sa prise de position du 27 août 2021, le Préposé a reconnu les clauses contractuelles types de l'UE comme base pour le transfert de données personnelles vers des pays tiers ne présentant pas un niveau de protection adéquat. Il a prévu des adaptations et des compléments pour que l'utilisation de ces données soit conforme au droit suisse.

Selon la loi suisse sur la protection des données, les données personnelles ne peuvent pas être transférées vers des pays ne disposant pas d'un niveau de protection des données adéquat. Des exceptions sont possibles si une protection adéquate dans le pays de destination peut être garantie, par exemple par contrat. Il convient d'examiner dans chaque cas d'application concret si des accords contractuels sont effectivement appropriés pour garantir une protection adéquate des données personnelles à transférer. À ce propos, le Préposé a publié sur son site Internet un guide permettant de vérifier l'admissibilité des transferts de données personnelles vers l'étranger.

Si une garantie contractuelle pour un transfert est envisageable, les clauses contractuelles types (CCT) adoptées par la Commission européenne dans sa décision d'exécution (UE) 2021/914 du 4 juin 2021 sont un outil efficace.

Dans sa prise de position du 27 août 2021, le Préposé a reconnu ces nouvelles clauses contractuelles types (y compris leurs modules) qui se réfèrent au Règlement général de l'UE sur la protection des données (RGPD), sous réserve qu'elles soient modifiées et complétées si nécessaire dans des cas d'espèce. Le Préposé explique à ce sujet qu'après avoir choisi le scénario correspondant au cas concret (l'exportateur et l'importateur de données peuvent être aussi bien responsables que sous-traitants), il faut déterminer à quel droit le transfert de données est soumis : uniquement au droit suisse de la protection des données ou à la fois au droit suisse et au droit européen de la protection des données. Cette distinction entraîne diverses adaptations du contrat, notamment en ce qui concerne l'autorité de surveillance compétente, le droit applicable aux droits contractuels et le for des litiges. Pour plus de détails, il convient de se reporter à la prise de position du Préposé consultable sur son site.

Conformément au droit en vigueur, le Préposé doit être informé de l'utilisation des clauses contractuelles types reconnues avant la communication des données. Cette obligation de notification disparaîtra avec l'entrée en vigueur de la nouvelle loi sur la protection des données.

Schéma d'examen de la licéité selon l'art. 6, al. 2, let. a, LPD

À la suite de sa prise de position du 8 septembre 2020 sur le bouclier de protection des données entre la Suisse et les États-Unis, le Préposé a publié un guide pour l'examen de la licéité de la communication transfrontière de données conformément à l'art. 6, al. 2, let. a, LPD. Il n'est pas licite de transférer des données à l'étranger si les garanties contractuelles et les mesures de protection supplémentaires sont insuffisantes.

Le guide publié par le Préposé sur son site Internet vise à faciliter l'examen, par les responsables des traitements, de la licéité des transferts de données à l'étranger. Il illustre, au moyen d'un schéma et d'un questionnaire, la procédure de transfert de données vers l'étranger dans les cas où le pays de destination ne dispose pas d'une législation assurant une protection adéquate et où cette carence doit donc être compensée ou éliminée par d'autres garanties suffisantes (art. 6, al. 2, let. a, LPD).

Si un pays figure sur la liste des États du Préposé en tant qu'État ne disposant pas d'un niveau de protection adéquat ou si la protection n'est pas applicable au transfert de données envisagé, l'exportateur doit, après analyse de son projet concret de transfert de données, prévoir d'autres mesures avec l'importateur, par exemple des dispositions contractuelles. D'une manière générale, il s'agira de clauses contractuelles types (CCT) (cf. article page de gauche).

En cas d'utilisation des clauses contractuelles types, il convient de vérifier si elles ne suffisent pas à elles seules, lorsque par exemple des règles non adéquates du droit applicable au partenaire contractuel prévalent. Dans ce cas, il faut examiner si les quatre garanties apportées par les droits fondamentaux (principe de légalité, principe de proportionnalité, possibilité de disposer de voies de droit et garantie de l'accès au juge) sont assurées par le droit étranger applicable. À titre de complément, le Préposé a joint à ce guide une liste de questions ciblées sur le droit des États-Unis, reposant sur les questionnaires de l'organisation non gouvernementale de Maximilian Schrems « My Privacy Is None Of Your Business » (NOYB).

Si toutes les garanties requises sont assurées par le droit auquel la partie contractante est soumise, les clauses contractuelles types sont suffisantes, sauf si d'autres mesures de protection contractuelles s'imposent. Il pourrait s'agir, notamment, de dispositions renforçant les droits des personnes concernées (p. ex. droit d'accès) ou de certaines mesures techniques constituant la condition à un transfert de données.

En revanche, si ces garanties ne figurent pas cumulativement dans la législation applicable au partenaire contractuel, l'exportateur doit envisager d'autres mesures de protection contractuelles, organisationnelles ou en particulier techniques. Si de telles mesures ne permettent pas de compenser l'absence de protection, le transfert de données à l'étranger est illégal et il faut immédiatement le suspendre ou y mettre fin.

Risques et conditions attachés à l'utilisation de nuages publics par les autorités

Pendant la période sous revue, le PFPDT s'est encore beaucoup préoccupé d'informatique en nuage. Invité à s'exprimer lors de consultations des offices et dans un groupe de travail de l'administration fédérale, il a souligné les risques et les conditions attachés à l'externalisation, par les autorités, du traitement de données personnelles à des fournisseurs de nuages publics.

En relation avec l'interpellation Andrey « Services informatiques en nuage. Adjudication de marchés publics à des entreprises américaines et chinoises » du 16 septembre 2021, le PFPDT a signalé au secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale (ChF) que même la gestion « fiduciaire » des services en nuage par des sociétés européennes telle qu'elle est envisagée n'exclut pas forcément des complications dans l'application de certaines dispositions légales étrangères, avec le risque d'un accès disproportionné des autorités. Il a ajouté qu'il fallait s'assurer que le fournisseur, en plus de garantir la sécurité des données, était en mesure de respecter le secret de fonction. Il a en outre rappelé qu'indépendamment du lieu visé, confier des données personnelles à des tiers accroît toujours les risques qui pèsent sur l'intégrité, la disponibilité et la confidentialité des données, d'où la nécessité de procéder à une analyse des risques.

Le PFPDT a aussi déclaré au TNI, à propos de l'interpellation Marti « Services en nuage de Microsoft » du 30 septembre 2021, que s'agissant des travaux en cours de l'administration, la décision de recourir ou non aux services en nuage de Microsoft ou d'autres fournisseurs ne pourrait être prise qu'après une analyse des bases légales, l'élaboration d'un plan de sécurité de l'information et de protection des données, et une analyse des risques (y compris ceux concernant la protection des données). Le Préposé souligne la nécessité d'examiner des offres concurrentes compte tenu du fait que le nuage accueillera potentiellement des textes, outre des données télémétriques et des données spécifiques aux utilisateurs. Dans ce contexte, il rappelle que le droit de la protection des données peut justifier l'imposition de mesures techniques visant à empêcher les accès disproportionnés des autorités du pays cible.

Le Préposé a par ailleurs participé, en tant que conseil, aux séances d'un groupe de travail ad hoc dirigé par la section du droit de la ChF sur le rapport relatif au cadre juridique de l'informatique en nuage. Ce rapport fait partie de la stratégie d'informatique en nuage de l'administration fédérale et vise à clarifier, sous l'angle du droit, l'utilisation par celle-ci de nuages publics. Cette clarification est particulièrement urgente vu la vitesse à laquelle les projets de l'administration fédérale fondés sur des solutions en nuage prennent forme.

À l'instar des autorités de protection des données des autres pays d'Europe, le PFPDT est en train de développer une jurisprudence concernant l'externalisation par les autorités de traitements de données personnelles, notamment à des fournisseurs américains de services en nuage public. Bien que ni le droit de l'Union européenne (UE) ni les arrêts de la Cour de justice de l'UE ne soient applicables en Suisse, le Préposé tient compte de l'évolution du droit européen dans l'élaboration de sa jurisprudence dans la mesure où il vise, pour l'application de la législation fédérale sur la protection des données, un niveau de protection comparable à celui de l'UE compte tenu des décisions d'adéquation mutuelles de l'UE et de la Suisse. À ce propos, notons que la présidente de la Commission européenne et le président des États-Unis ont fait part fin mars 2022 de leur intention commune de remplacer bientôt par une réglementation améliorée le régime de transferts de données entre l'UE et les États-Unis dit « Privacy shield », invalidé par la Cour de justice de l'UE (cf. 28e rapport d'activités, Accent II).

SCHREMS II

Comité européen de la protection des données (CEPD), sous-groupe Borders, Travel & Law Enforcement (BTLE)

Le Préposé met à profit sa présence au sein du Comité européen de la protection des données (CEPD) pour s'exprimer, principalement sur les questions relatives à Schengen, et pour échanger des informations avec les autres autorités européennes. Au cours de la période sous revue, l'accent a été mis sur les répercussions de Schrems II et sur la réaction des autorités de protection des données quant à cette jurisprudence.

Au cours des six premiers mois de la période sous revue, le Préposé a surtout été actif au sein du sous-groupe Borders, Travel & Law Enforcement. Ce groupe de travail s'est intensément penché sur le cas Schrems II et a élaboré les recommandations au nom du CEPD. En juin 2021, le CEPD a adopté en séance plénière la version finale des « recommandations sur les mesures supplémentaires à la suite de l'arrêt Schrems », après avoir procédé à une consultation publique. Ces recommandations aideront les responsables du traitement et les sous-traitants, qui agissent en tant qu'exportateurs de données, à lister et mettre en œuvre les mesures supplémentaires appropriées. Ces mesures peuvent être requises pour garantir aux données personnelles transférées vers des pays tiers, un niveau de protection fondamentalement équivalent.

Le 18 juin 2021, le Préposé a publié un guide, basé sur le droit suisse, aidant à l'examen de l'admissibilité des transferts de données à l'étranger (cf. article précédent « Schéma d'examen de la licéité selon l'art. 6, al. 2, let. a, LPD »).

Principe de la transparence

2.1 Généralités

La loi sur la transparence vise à promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration. À cette fin, elle contribue à l'information du public en garantissant l'accès aux documents officiels (cf. art. 1 LTrans). En permettant la traçabilité de l'action administrative, le principe de transparence vise à promouvoir la confiance dans l'État et les autorités, augmentant ainsi l'acceptation de l'action étatique.

Les chiffres fournis par l'administration fédérale concernant les demandes d'accès à des documents officiels reçues en 2021 confirment le fort besoin des médias et de la société quant à une information spécifique et transparente. Ainsi, durant l'année sous revue, les demandes d'accès déposées auprès des autorités fédérales ont été à nouveau plus nombreuses que l'année précédente. De plus, au cours de cette deuxième année de pandémie, les demandes, pour certaines complexes et volumineuses, concernaient dans près d'un cas sur quatre des documents officiels liés au COVID-19. Le traitement des demandes d'accès a souvent mobilisé d'importants moyens, surtout lorsqu'une coordination entre offices ou départements a été nécessaire. Globalement, il ressort que la mise en œuvre du principe de transparence en période de pandémie pose un défi majeur. Les chiffres suivants (cf. chap. 2.2) confirment également pour l'année sous revue les tendances constatées ces dernières années – augmentation constante des demandes d'accès et proportion élevée des cas dans lesquels l'accès est entièrement accordé.

Si les demandeurs ou les tiers concernés ne sont pas d'accord avec l'accès que les autorités envisagent d'octroyer, la loi sur la transparence leur offre la possibilité de déposer une demande en médiation auprès du Préposé. Là aussi, une tendance claire se dégage : le Préposé a reçu 149 demandes en médiation au cours de l'année sous revue, ce qui représente une augmentation de 60 % par rapport à l'année précédente.

L'objectif de la procédure de médiation est de parvenir rapidement à un accord entre les parties. Les mesures introduites à cet effet lors de l'essai pilote de 2017, et notamment la primauté des procédures de médiation orales, ont à nouveau fait leurs preuves en 2021. L'évaluation des demandes en médiation traitées au cours de l'exercice 2021 montre que dans les cas où une médiation orale a pu être organisée, une solution à l'amiable a été trouvée dans 67 % des cas. En revanche, dans les 40 procédures de médiation dans lesquelles la médiation orale était impossible en raison de la pandémie, un accord n'a pu être trouvé que dans 5 % des cas. Le 13 janvier 2021, compte tenu de la situation épidémiologique tendue, le Conseil fédéral a introduit les obligations de travailler à domicile et de limiter à cinq personnes les rassemblements dans l'espace public entre autres. Cette injonction a eu des répercussions directes sur la manière dont les procédures de médiation ont été menées. Ainsi, entre janvier et juin 2021,

le Préposé n'a pas pu organiser les séances de médiation en présence des parties. En conséquence, de nombreux cas ont dû faire l'objet d'une procédure de médiation écrite ; cela a non seulement entraîné une diminution du nombre de solutions à l'amiable au cours de l'année sous revue, mais aussi un allongement de la durée de traitement des procédures de médiation et, par contrecoup, un retard dans le règlement des procédures (cf. chap. 2.3).

Les chiffres ainsi analysés montrent clairement que la tenue de séances de conciliation in situ, en présence des parties concernées, contribue à un règlement rapide des procédures. Toutefois, le nombre de demandes en médiation ayant constamment augmenté depuis des années et du fait de leur complexité croissante, le Préposé dépasse le délai légal de 30 jours pour une part croissante des procédures. Il estime à ce propos que sans ressources supplémentaires, cette évolution négative s'accentuera et que le traitement rapide des procédures exigé par le législateur continuera d'être entravé (cf. à ce propos les informations plus détaillées figurant au chap. 2.3).

Contrats d'acquisition de vaccins contre le COVID-19

Consécutive à une demande en médiation ouverte au cours de l'année sous revue, la recommandation du Préposé du 18 janvier 2022 a largement suscité l'attention des médias. Le Préposé a recommandé à l'OFSP de consulter les entreprises pharmaceutiques concernées et d'accorder l'accès aux contrats d'acquisition de vaccins contre le COVID-19 dans le respect du principe de proportionnalité. Dans sa recommandation, dûment motivée, le Préposé a précisé que, devant revenir sur les exceptions justifiant le report de l'accès, il était tenu de prendre en compte l'évolution des circonstances. L'OFSP ayant lui-même expliqué que la pénurie initiale de vaccins avait entre-temps disparu, le Préposé a estimé qu'il n'y avait plus de motif suffisant pour différer davantage le traitement des demandes d'accès. Il a également tenu compte du fait que la consultation des entreprises pharmaceutiques nécessiterait probablement des délais supplémentaires. Cette recommandation du Préposé est conforme à la décision du Parlement de ne pas inscrire dans une loi spéciale, souhaitée par le Conseil national, l'obligation de publication pour les contrats de vaccins. En l'absence de disposition légale spécifique, c'est la loi sur la transparence qui s'applique, ainsi qu'il ressort d'ailleurs des délibérations du Conseil des États. En application de cette loi, le Préposé a recommandé d'accorder l'accès que l'OFSP avait différé.

2.2 Demandes d'accès – Nouvelle hausse en 2021

Selon les chiffres communiqués par les autorités fédérales, 1385 demandes d'accès ont été déposées au cours de l'année sous revue (contre 1193 en 2020), ce qui correspond à une augmentation de 16 % par rapport à 2020. Dans 694 cas (50 %), les autorités ont accordé un accès intégral (contre 610, soit 51 % en 2020), tandis que dans 324 cas (23 %), un accès limité ou différé aux documents a été autorisé (année précédente : 293 demandes, soit 25 %). Dans 126 cas (9 %), l'accès a été totalement refusé (contre 108, soit 9 % en 2020). Selon les indications des autorités, 48 demandes d'accès ont été retirées (contre 35, soit 3 % en 2020), 78 demandes étaient encore en suspens à la fin 2021 et 115 ne correspondaient à aucun document officiel.

L'augmentation du nombre de demandes d'accès tient probablement aussi au fait que par l'intermédiaire des médias, la population acquiert une meilleure connaissance du principe de transparence et qu'elle en exploite aussi de plus en plus activement les possibilités. Cette tendance devrait se poursuivre dans les années à venir.

Le besoin d'information et de transparence apparu dans le sillage des mesures de lutte contre la pandémie de COVID-19 a aussi contribué à l'augmentation du nombre des demandes d'accès. Les autorités ont établi une évaluation statistique des demandes d'accès liées au COVID-19 et l'ont transmise au Préposé, en même temps que les informations à communiquer chaque année (cf. Statistiques Demandes d'accès 2021 liées au Corona). D'après les chiffres des autorités fédérales, sur 1385 demandes d'accès, 336 était en rapport avec le coronavirus (soit 24 %) : l'accès complet a été accordé dans 121 cas (36 %), soit moins souvent que dans la statistique générale. Toujours dans le domaine des demandes liées à la pandémie, les autorités ont accordé un accès partiel ou différé dans 131 cas (39 %), soit plus souvent, et un refus complet dans 13 cas (4 %), soit un pourcentage de moitié inférieur à celui de la statistique générale. 18 demandes d'accès ont été retirées, 29 étaient encore en suspens à la fin 2021 et dans 24 cas, la demande ne correspondait à aucun document officiel. Il est permis de penser que l'analyse sociale des mesures prises par les autorités contre la pandémie se poursuive au-delà de la maîtrise escomptée de la crise sanitaire, de sorte qu'en 2022, les demandes d'accès et demandes en médiation liées à la pandémie devraient se maintenir.

En résumé, le Préposé constate que depuis 2015, un accès complet aux documents est accordé dans au moins 50 % des cas et que les refus d'accès complets se sont stabilisés au fil des ans à près de 10 %.

Départements et offices fédéraux

En 2021, pour la deuxième année consécutive, la pandémie de COVID-19 a focalisé l'attention des médias et de la société sur certaines unités administratives. Du fait de leurs tâches, le DFI et le DDPS ont reçu un grand nombre de demandes d'accès. Dans le cas du DFI, 63 % des demandes, à un niveau supradépartemental, concernaient l'accès à des documents officiels en rapport avec le COVID-19.

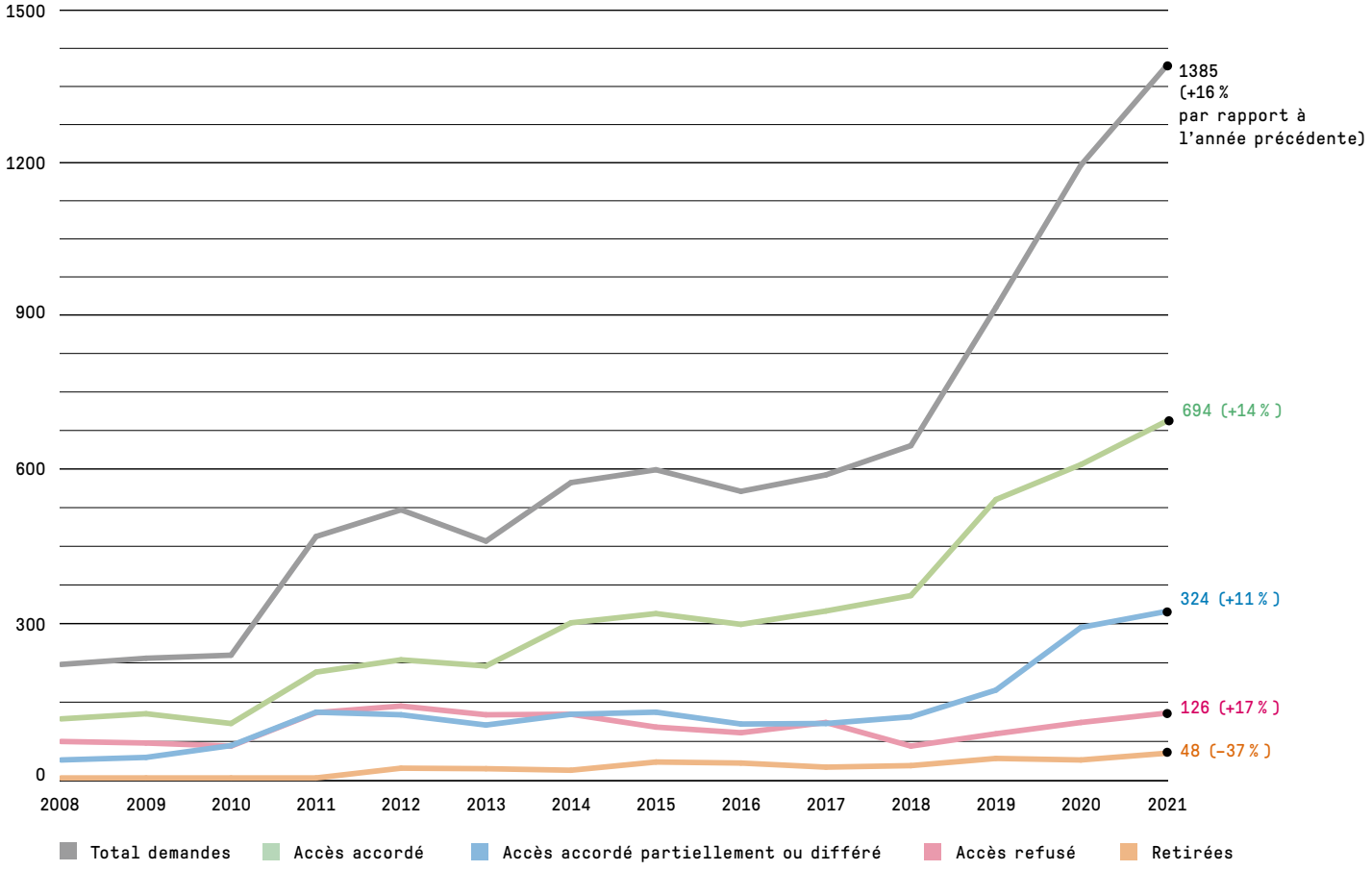
Selon les autorités, certaines de ces demandes étaient à la fois très volumineuses et très complexes. Par ailleurs, de nombreux cas ont nécessité une coordination lourde entre offices ou entre départements. Pour ces autorités, le traitement des demandes a représenté une charge de travail accrue par rapport à la période précédant la pandémie et, comme nous l'avons déjà mentionné, cette situation pourrait perdurer en 2022.

À l'échelon des offices, c'est l'OFSP qui a signalé le plus de demandes (251) au cours de l'année sous revue, dont 217 concernaient des documents en rapport avec le COVID-19. Viennent ensuite l'OFSPO (172), swissmedic (72) et l'OFEV (64). En ce qui concerne les départements, le DFI (422), le DDPS (281) et le DFAE (156) arrivent en tête. 13 autorités déclarent n'avoir reçu aucune demande d'accès en 2021. Le

Préposé lui-même en a reçu 16, dont 7 auxquelles l'accès a été entièrement accordé ; dans deux cas, l'accès a été partiellement accordé ou reporté, et dans deux autres cas, entièrement refusé. 5 demandes d'accès étaient encore pendantes à la fin de l'année 2021.

En 2021, les émoluments perçus pour l'accès à des documents officiels ont atteint un montant de 14 924,90 francs, légèrement inférieur à celui de l'année précédente (15 189,30 francs). Alors que le DFAE, l'OFEV, les Services du Parlement et le Ministère public de la Confédération n'ont prélevé aucun émolument, les cinq autres départements et la Chancellerie fédérale ont facturé aux demandeurs une partie du temps consacré au traitement des demandes d'accès (DFI : 7665,20 francs ; DEFR : 4052,70 francs ; ChF : 1150 francs ; DDPS : 950 francs ; DFF : 750 francs ; DFJP : 357 francs). Signalons que 19 seulement des 1385 demandes déposées ont donné lieu à une perception d'émoluments, contre 25 l'année précédente, ce qui représente une diminution tant du nombre de cas que du montant total des émoluments. Cela 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. Cette pratique de l'administration basée sur la possibilité de consulter gratuitement les documents officiels sera inscrite dans la loi. Le 1er décembre 2021, après le Conseil national, le Conseil des États lui aussi est entré en matière sur une initiative parlementaire à ce propos. Selon cette

Graphique 1 : Demandes d'accès – évolution depuis 2008



initiative, les demandes ne devront être à l'avenir payantes que si leur traitement entraîne un surcroît de travail particulièrement important pour les autorités. Le Parlement doit maintenant décider de la forme concrète et de la mise en œuvre du principe de gratuité et des éventuelles exceptions en matière d'accès aux documents officiels.

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 5010 heures en 2020 à 5562,35 heures en 2021.

Les données communiquées par l'OFSP montrent clairement que le temps consacré par les autorités au traitement des demandes d'accès correspond en partie seulement au temps effectivement nécessaire. En plus du temps de travail de 208,5 heures

indiqué ponctuellement par les unités spécialisées compétentes de l'OFSP et du soutien juridique apporté par sa conseillère en relations publiques à hauteur de 40 pour cent de poste, l'OFSP a signalé la mise en place d'une structure d'exécution propre ainsi que de processus spécifiques pour le traitement des nombreuses demandes d'accès liées au COVID-19. Selon les indications de l'OFSP, le temps de travail a été extrêmement élevé au cours de l'année sous revue et a représenté au moins 3,9 postes à plein temps. Il en va certainement de même pour d'autres unités de l'administration fédérale.

Le temps consacré à la préparation des procédures de médiation a lui aussi augmenté : 864,6 heures (contre 569 en 2020, 473 en 2019, 672 en 2018 et 914 en 2017).

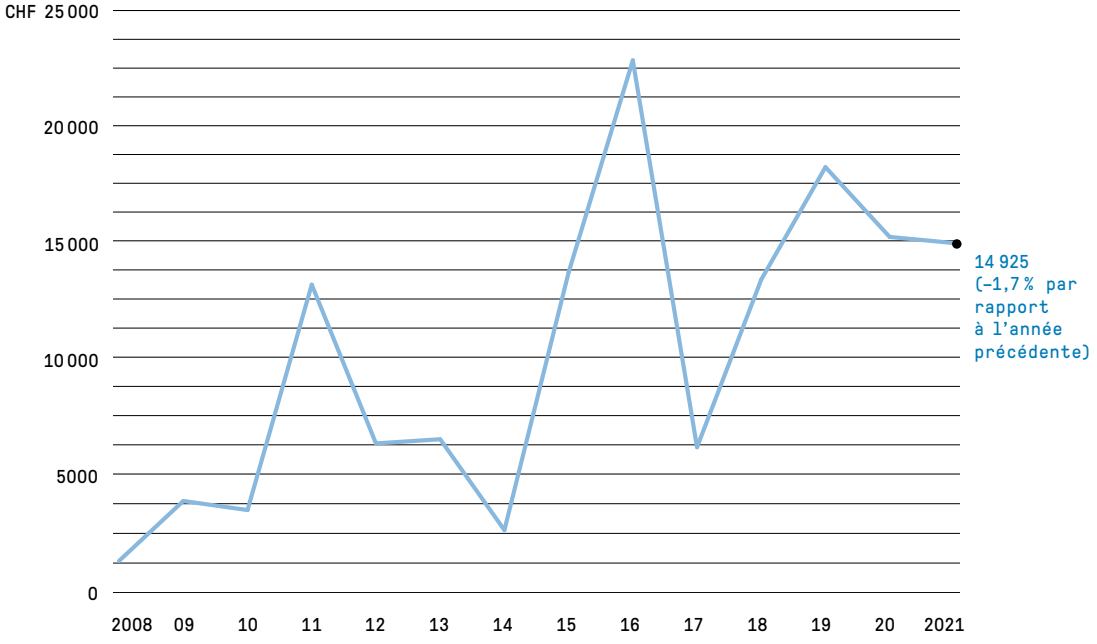
Services du Parlement

Les Services du Parlement ont déclaré avoir reçu une demande d'accès. Elle a été approuvée et l'accès aux documents demandés a été entièrement accordé.

Ministère public de la Confédération

Le Ministère public de la Confédération a déclaré avoir reçu 8 demandes en 2021. L'accès a été refusé entièrement dans 4 cas et partiellement accordé dans 1 cas. Les 3 autres demandes ne correspondaient à aucun document officiel.

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



2.3 Procédures de médiation – Nette augmentation des demandes

En 2021, le Préposé a reçu 149 demandes en médiation, ce qui correspond à une augmentation de 60 % par rapport aux 93 demandes reçues en 2020. La plupart de ces demandes émanaient de journalistes (53) et de particuliers (49). Ces chiffres appellent le constat suivant : sur les 565 cas dans lesquels la demande a été entièrement ou partiellement rejetée par la Confédération ou repoussée, ou encore ne correspondait à aucun document officiel, 149 (26 %) demandes en médiation ont été déposées, dont 31 (21 %) concernaient des documents officiels en rapport avec le COVID-19.

139 demandes en médiation ont été réglées en 2021. 126 avaient été déposées en 2021 et 13 au cours de l'année précédente. Les parties ont trouvé un accord dans 50 cas. Le Préposé a émis 49 recommandations, ayant permis de régler 63 cas dans lesquels aucune solution à l'amiable entre les parties ne semblait se dessiner.

Aux cas réglés s'ajoutent 7 demandes en médiation déposées hors délai, 17 qui ne remplissaient pas les conditions d'application de la loi sur la transparence et 2 qui ont été retirées.

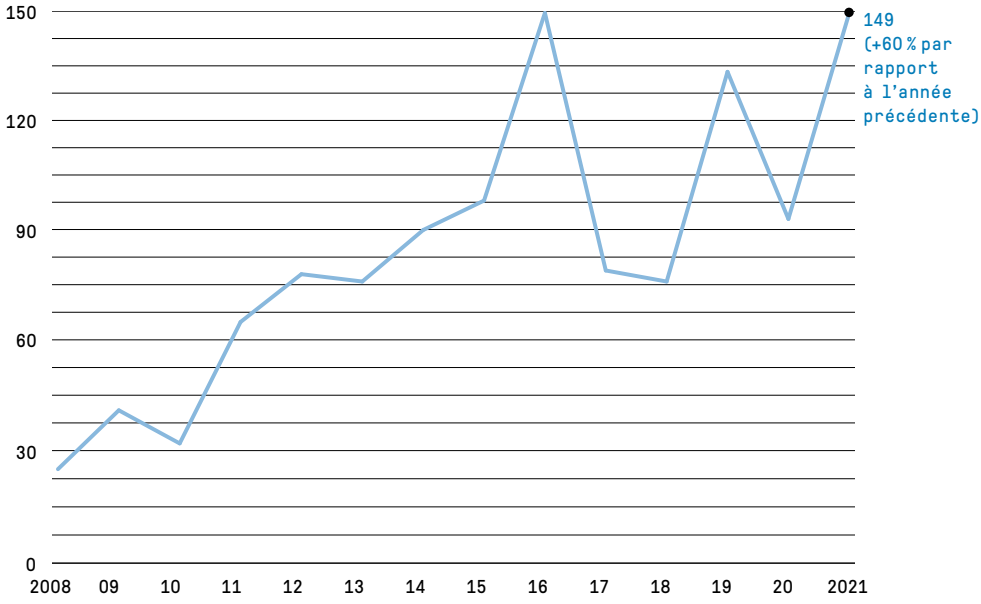
À la fin de l'année, 8 procédures de médiation ont été suspendues en accord avec les parties ou à leur demande.

Proportion des solutions amiables

Les solutions à l'amiable présentent de nombreux avantages, dont ceux d'accélérer la procédure d'accès aux documents et de jeter les bases d'une collaboration future entre les personnes impliquées dans la séance de médiation.

L'efficacité des mesures instaurées en 2017 et des procédures de médiation orales transparaît régulièrement dans la proportion de solutions amiables par rapport aux recommandations. Au cours de l'année sous revue, 50 solutions amiables ont été trouvées et le Préposé a émis 49 recommandations réglant 63 cas. Les solutions amiables représentent donc 44 % des procédures de médiation. Il convient toutefois d'apporter quelques précisions à ce sujet : pour aboutir à une solution amiable, il faut que la procédure de médiation puisse avoir lieu. Ainsi, durant l'année sous revue, sur les 45 procédures menées, 30 (67 %) ont abouti à un accord. Comme nous l'avons déjà relevé au chap. 2.1, du fait des mesures mises en œuvre pour lutter contre le COVID-19, il a été impossible, entre janvier et juin 2021, soit dans 40 cas, d'organiser les

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



séances de médiation en présence des parties. Ceci a eu un réel impact sur la part des solutions amiables : seules deux des procédures écrites (5 %) ont abouti à un accord.

En conclusion, il convient de souligner l'efficacité constante des procédures de médiation orales qui permettent l'émergence de solutions consensuelles. De l'avis du Préposé, il convient de continuer à privilégier et à encourager ce type de procédure par rapport aux procédures écrites. La tenue de séances de médiation en présentiel se révèle profitable pour toutes les parties à la procédure. Dans certains cas, celles-ci ont d'ailleurs demandé, compte tenu des mesures sanitaires, une suspension de la procédure jusqu'au moment où les négociations orales seraient à nouveau possibles.

Remarque : toutes les recommandations émises au cours de l'année sous revue peuvent être consultées sur le site Internet du Préposé.

Tableau 1: Solutions amiables

2021 (Corona)	**44 %**
2020 (Corona)	34 %
2019	61 %
2018	55 %

Durée des procédures de médiation

Le tableau 2 (page suivante) est divisé en trois 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 de médiation, 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 congés, 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 en outre que 42 % des procédures réglées en 2021 l'ont été dans le délai réglementaire de 30 jours, 51 % dans un délai compris entre 31 et 99 jours, et 7 % en l'espace de 100 jours ou davantage.

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. Durant l'année sous revue, lorsque la procédure s'est terminée par un accord, le délai de 30 jours a été respecté dans 60 % des cas.

En raison du nombre élevé de demandes en médiation remises au Préposé en 2021, il était avéré dans certains cas, dès la réception de la demande, que le délai de 30 jours ne pourrait pas être tenu : compte tenu des effectifs disponibles pour le traitement des demandes en médiation, la séance de médiation devait alors être fixée d'emblée de telle sorte que le délai était déjà dépassé à la date choisie pour la séance.

Il convient en outre de noter que sur les 59 demandes en médiation traitées dans le délai de 30 jours, dans 31 cas seulement (53 %) la procédure de médiation a été réglée par un accord ou une recommandation, donc au terme d'un examen matériel de l'objet de la médiation. Dans les 28 autres cas (47 %), il n'y a pas eu d'appréciation matérielle quant au fond ; il s'agissait en particulier de cas qui sortaient du champ d'application de la loi sur la transparence ou pour lesquels les conditions formelles d'ouverture d'une procédure de médiation n'étaient pas remplies.

Comme nous l'avons déjà mentionné, aucune séance de conciliation n'a pu être organisée en présentiel de janvier à juin 2021 en raison de la pandémie. De ce fait, les procédures de

médiation menées pendant cette période ont été très peu nombreuses à aboutir à une solution amiable (dans seulement 5 % des cas). Lorsqu'aucun accord n'est trouvé, le Préposé doit établir une recommandation écrite. La mise en œuvre d'une procédure de médiation par écrit et l'élaboration d'une recommandation entraînent en général une charge de travail nettement plus importante. Il en résulte une tendance à l'allongement de la durée de traitement des procédures en question, ce qui se répercute sur toutes les procédures suivantes et sur leur durée de traitement. Dans le même contexte, les réglementations introduites du fait de la pandémie ont aussi entraîné un allongement de la durée des procédures, et donc un retard dans le traitement des dossiers.

S'il y a déjà un retard dans le traitement des procédures de médiation, chaque nouvelle demande reçue contribue à accroître le nombre des traitements en attente. Au cours de l'année sous revue, dans 4 cas seulement (7 %), le Préposé a pu faire parvenir aux parties concernées la recommandation écrite dans les 30 jours suivant la réception de la demande, et donc dans le délai légal.

Les autres dépassements de délais ont été principalement dus à l'absence des personnes ou des autorités concernées (vacances, maladie, voyages), au grand nombre de tiers impliqués dans la procédure ou à la complexité juridique du cas. Ces motifs s'appliquent aussi aux 9 cas dont le traitement a duré plus de 100 jours. Parmi les difficultés supplémentaires ayant mené à un dépassement figurent aussi la tenue de consultations à l'étranger, les nombreux efforts de négociation entre les parties et la pléthore de documents ou la multitude des individus concernés. Le traitement de ces cas étant souvent particulièrement complexe, le Préposé peut prolonger d'une durée raisonnable le délai réglementaire, conformément à l'art. 12a de l'ordonnance sur le principe de la transparence dans l'administration (OTrans ; RS 152.31).

Le législateur a conçu la procédure de médiation comme une procédure informelle et non préjudicielle de règlement amiable des différends. L'expérience montre cependant que pour un requérant ou un tiers concerné, faire

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	Période 2021
dans un délai de 30 jours	11 %	59 %	50 %	57 %	43 %	42 %
de 31 à 99 jours	45 %	37 %	50 %	38 %	30 %	51 %
plus de 100 jours	44 %	04 %	00 %	05 %	27 %	7 %

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

appel à un avocat dès la demande d'accès ou en procédure de médiation ne contribue pas à l'obtention de solutions simples, rapides et pragmatiques.

Alors que les dépassements du court délai de 30 jours dans les cas complexes et les procédures multipartites (c'est-à-dire plusieurs tiers concernés) sont considérés comme inhérents au système en raison de la possibilité légale de prolongation, les dépassements de délai qui s'accumulent à nouveau en raison uniquement d'un manque d'effectifs constituent, sur le plan juridique, des retards injustifiés.

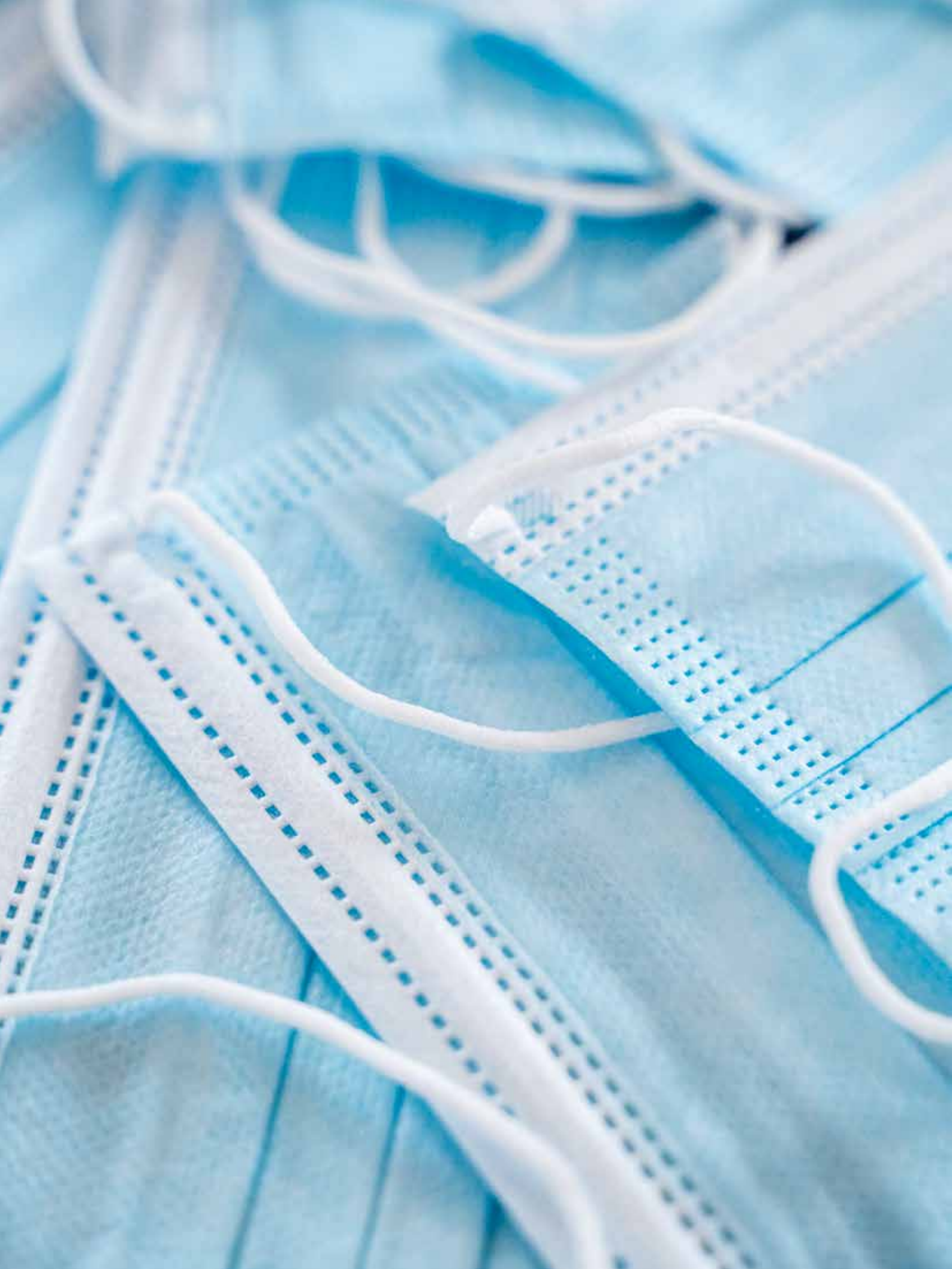
Nombre de cas pendants

Les chiffres ci-dessous (cf. tableau 3) indiquent le nombre de cas pendants à la fin de chaque année. Fin 2021, il y avait 27 procédures de médiation pendantes, dont 8 suspendues (3 datant de 2019, 1 de 2020 et 4 de l'année sous revue). 14 cas ont pu être réglés avant la mise sous presse du présent rapport.

Il semble que d'ici la fin de l'exercice prochain, la durée de traitement continuera d'augmenter, qu'il y aura une nouvelle hausse des dépassements juridiquement injustifiés du délai ordinaire et que le nombre de cas pendants continuera aussi d'augmenter.

Tableau 3: Procédures de médiation pendantes

Fin 2021	**27 (dont 14 terminées à la mise sous presse et 8 suspendues)**
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 Processus législatif

CONSULTATION DES OFFICES

Révision de la loi sur le renseignement

La loi fédérale sur le renseignement du 25 septembre 2015 (LRens ; RS 121) est actuellement en cours de révision. Le projet de révision remis au Préposé dans le cadre de la consultation des offices prévoyait une nouvelle extension du champ des informations exclues de la loi sur la transparence.

En application de l'actuel article 67 LRens, la loi sur la transparence ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations au sens de la LRens. Cette notion est clairement délimitée par le chapitre 3 de la loi sur le renseignement. La nouvelle mouture de cet article envisage désormais d'exclure l'ensemble des données de renseignements. Du point de vue du Préposé, le Service de renseignement de la Confédération (SRC) tente, par la modification de cette disposition, une fois encore, de restreindre la portée de la loi sur la transparence en étendant le champ des informations exclues de celle-ci. Avec cette nouvelle formulation, la majeure partie de l'activité du SRC serait ainsi soustraite à la loi sur la transparence ce qui irait à l'encontre de la volonté du législateur qui a introduit la loi sur la transparence afin de promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration.

Le Préposé s'y est fermement opposé entre autres car, les exceptions des articles 7 à 9 LTrans – en particulier les exceptions permettant de protéger la sûreté intérieure ou extérieure de la Suisse (art. 7 al. 1 let. c LTrans), les intérêts de la Suisse en matière de politique extérieure (art. 7 al. 1 let. d LTrans) et les données personnelles (art. 7 al. 2 LTrans) – trouvent déjà application et offrent une protection suffisante et adéquate.

À l'issue de la consultation des offices, le SRC, après avoir dans un premier temps maintenu sa position, a finalement informé le Préposé qu'il abandonnait la modification de l'actuel art. 67 LRens.

Le PFPDT

3.1 Tâches et ressources

Pandémie

Les projets de traitement de données dans le cadre de la lutte contre pandémie, réalisés dans de courts délais en raison de la crise, ainsi que la demande croissante de documents officiels ont extrêmement sollicité l'ensemble du personnel dans cette deuxième année de COVID-19.

En tant qu'unité administrative subordonnée à la Chancellerie fédérale (ChF), le PFPDT a mis en œuvre toutes les prescriptions du Conseil fédéral visant à protéger la santé du personnel. Avec la levée en février 2022 par le Conseil fédéral de l'obligation du télétravail pour le personnel de la Confédération, le PFPDT a réduit le travail à domicile à compter du 1er mars 2022 aux proportions prévues par le modèle de temps de travail souple. Depuis, les rencontres personnelles ont pu reprendre, ce qui favorise notamment 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 s'expliquent d'une part par l'entrée en vigueur, en 2006, de la loi sur la transparence (le Conseil fédéral n'ayant jamais approuvé les postes prévus pour l'application de celle-ci, 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 PFPDT la création de 9 à 10 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 l'entrée en vigueur de cette loi le 1er mars 2019, le Conseil fédéral a attribué au Préposé 3 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 PFPDT a demandé au Conseil fédéral la création des 6 postes à plein temps restants, dans la perspective de l'entrée en vigueur, prévue alors en 2022, de la LPD révisée. L'autorisation de ces postes a eu lieu dans le cadre de l'évaluation globale des ressources. Après l'entrée en vigueur de la nouvelle législation, le Conseil fédéral ne transmettra plus que les nouvelles demandes de ressources du PFPDT aux Chambres fédérales pour décision.

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
2022	**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 2021 au 31 mars 2022, les ressources en person-

nel dont dispose le PFPDT pour la protection des données ont été affectées de la manière suivante :

Tableau 5: Prestations en matière de protection des données

Conseil Privés	22,1 %	
Conseil Confédération	18,9 %	
Collaboration avec les cantons	1,4 %	
Collaboration avec des autorités étrangères	13,4 %	
Total conseil		**55,8 %**
Surveillance	16,8 %	
Certification	0,1 %	
Registre de données	0,4 %	
Total surveillance		**17,3 %**
Information	13,1 %	
Formation/Conférences	3,1 %	
Total information		**16,2 %**
Législation	10,7 %	
Total législation		**10,7 %**
Total protection des données		**100,0 %**

Conseil

Comme indiqué dans le chapitre introductif « Défis actuels », le PFPDT est confronté à une demande élevée constante dans le domaine du conseil en raison de la nécessité d'accompagner les projets numériques d'envergure. Les ressources en personnel consacrées au conseil ont atteint 56 % pendant l'année sous revue. Selon le planning de contrôle du Préposé pour l'année 2022, le suivi de sept 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 PFPDT 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 en moyenne à 48 demandes et 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 nLPD prévoit, pour le PFPDT aussi, une obligation élargie de traiter matériellement les requêtes individuelles de la population suisse.

Étant donné que les « 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

Santé et secteur du travail	3
Commerce et économie	3
Douane	1
Total	7

Surveillance

Le dynamisme des applications fondées sur l'informatique en nuage impose aujourd'hui une exécution rapide des contrôles. Cette accélération et la nécessité croissante d'allier compétences juridiques et compétences 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 %. En 2021, elle était de 17,3 %. Selon le plan de contrôle 2022, 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 LPD a accru les attentes du public.

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 PFPDT 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 PFPDT 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. Le Conseil fédéral a d'ailleurs aussi validé les 6 postes restants dédiés à la mise en œuvre de la LPD (cf. supra).

Participation aux délibérations de commissions et auditions par les commissions parlementaires

- En avril 2021, la Commission des institutions politiques du Conseil national (CIP-N) a invité le Préposé à s'exprimer sur l'allégement des mesures anti-COVID pour les personnes vaccinées. Le même mois, la Commission des transports du Conseil national a consulté le PFPDT à propos de la révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.
- Fin octobre 2021 et mi-janvier 2022, les CIP des deux chambres ont invité le Préposé à trois séances relatives à la révision de la LPD et de ses ordonnances d'application.
- En octobre, la Délégation des Commissions de gestion a entendu le PFPDT sur la présentation d'un rapport concernant sa jurisprudence relative à l'art. 64 de la loi sur le renseignement.
- En novembre 2021, la CIP-N l'a entendu sur le budget 2022 et sur le plan financier 2023–2025.
- À la fin de la période, la Commission de la sécurité sociale et de la santé publique du Conseil des États a sollicité le Préposé à deux reprises sur la question de Swisstransplant.
- Et en février 2022, la sous-commission DFJP / ChF de la Commission de gestion du Conseil national a effectué une visite du service d'une demi-journée, laquelle a dû avoir lieu dans les locaux du Palais fédéral en raison de la pandémie.

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 pour ses activités, d'une latitude considérable. La tâche principale du PFPDT 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.

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

L'année sous revue a été marquée non seulement par la pandémie mais aussi et surtout par l'augmentation des demandes en médiation (cf. ch. 2.2). La preuve a été faite une fois de plus que les 4,4 postes affectés au domaine de direction Principe de la transparence ne suffisent pas pour accomplir les tâches dans le respect de la loi. Comme on l'a vu plus haut, le Conseil fédéral, contrairement à ce qu'il dit dans le message, n'a toujours pas approuvé les postes dont le PFPDT a besoin pour accomplir ses tâches découlant de la loi sur la transparence.

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, avec des retards à la clé. Le nombre et la complexité des demandes ne diminuant pas, le PFPDT dépasse le délai légal de traitement de 30 jours dans un nombre croissant de dossiers.

Comme la hausse du nombre de demandes devrait se poursuivre en 2022 et au-delà, la situation a peu de chances de s'arranger si l'effectif n'augmente pas. L'accélération des procédures visée par le législateur n'est donc plus garantie.

S'agissant du principe de la transparence, c'est aussi aux autorités politiques qu'il appartient d'attribuer des ressources au PFPDT pour l'exécution de ses tâches de médiation et de conseil.

Compte tenu de ces éléments, le Préposé a défini pour chaque groupe de prestations les objectifs ci-après, déterminants pour le calcul des ressources (cf. tableau 7) :

Tableau 7: Objectifs du PFPDT

Groupes de prestations	Objectifs de résultats
Conseil	Le PFPDT développe une présence adaptée aux attentes pour les conseils aux particuliers et pour l'accompagnement des projets de l'économie et des autorités fédérales portant sur des données sensibles, au moyen d'instruments adaptés au numérique.
Surveillance	Le PFPDT développe une densité plausible de contrôles.
Information	Le PFPDT sensibilise le public de manière proactive aux risques du numérique liés aux technologies et aux applications. Il dispose d'un site web moderne et facile d'accès. Les déclarations doivent pouvoir être transmises au PFPDT de manière sûre, simple et à tout moment via des portails de déclaration.
Législation	Le PFPDT exerce une influence précoce et active sur toutes les normes et les réglementations spéciales relatives à la protection des données qui sont élaborées sur les plans national et international. Il aide les milieux concernés à formuler des règles de bonnes pratiques.

3.2 Communication

Principaux thèmes des activités de communication

Déjà dominants tout au long de la période de référence précédente, les thèmes liés à la pandémie ont également été très présents durant l'année sous revue. Les questions adressées au Préposé ont toutefois moins porté sur le traçage des contacts que sur la conception et l'utilisation du certificat COVID ainsi que sur l'application SwissCovid. Dans ce contexte, le Préposé et ses spécialistes ont une nouvelle fois été très sollicités. Ils se sont engagés avec succès en faveur d'un certificat light peu gourmand en données et ne contenant aucune donnée relative à la santé. À cela s'est ajoutée l'affaire du site web mesvaccins.ch, que l'exploitant a dû fermer en raison de failles de sécurité. Globalement, les thèmes liés au coronavirus ont représenté une grande partie des activités de communication.

Les fuites de données dans les secteurs les plus divers – souvent révélées par des réseaux de journalistes d'investigation – ont constitué un autre thème majeur. Elles ont concerné les réseaux sociaux ainsi que des plateformes présentant un grand intérêt public, par exemple en lien avec les transports publics, le don d'organes ou les implants mammaires. En outre, nous avons reçu de nombreux signalements de cyberattaques visant des entreprises. Nous avons donc intensifié nos échanges avec le Centre national pour la cybersécurité (NCSC). L'obligation d'annoncer au Préposé les fuites de données sera effective dès l'entrée en vigueur de la nouvelle loi fédérale sur la protection des données (cf. Accent I).

La surveillance apparaît également comme un sujet d'intérêt, que ce soit dans le monde du travail, dans le secteur privé, le commerce de détail ou par le truchement de logiciels espions étatiques. Les thèmes tels que le tracking (comportement en matière de mobilité, de navigation sur Internet ou d'achat) et le développement de systèmes de reconnaissance biométrique qui espionnent la population à l'aide d'algorithmes (p. ex. Clearview) constituent un domaine dynamique suscitant encore et toujours l'intérêt des médias. En outre, les questions en lien avec la protection des données restent primordiales dans les nombreux projets de transition numérique de l'administration fédérale et de l'économie privée.

Au cours de l'année sous revue, le Préposé et le secteur Communication ont traité au total quelque 550 demandes émanant des médias et de diverses organisations.

Intérêt croissant de la part des médias et du public

Notre veille média, qui s'appuie sur une sélection de médias suisses et des principales publications de la presse internationale, a recensé plus de 6000 articles, contre environ 4000 au cours de l'année précédente. Une augmentation confirmant la tendance déjà constatée, à savoir l'intérêt croissant pour la protection des données et l'autodétermination informationnelle qui se traduit par une couverture médiatique plus large. D'une manière générale, le nombre d'articles concernant le coronavirus a légèrement reculé et représente encore environ un tiers des publications observées. En outre, les journalistes se sont concentrés sur les thèmes en lien avec la surveillance, la transmission des données et la réglementation des géants de la tech (GAFAM), ainsi que le cloud, la cybersécurité, l'intelligence artificielle et le big data.

Par ailleurs, nous avons constaté une augmentation des articles basés sur des documents obtenus en vertu de la loi sur la transparence.

Le nombre de demandes et de questions soumises au Préposé par les entreprises et les particuliers a également augmenté. Le PFPDT a traité quelque 6600 demandes par courrier électronique, courrier postal ou hotline téléphonique (contre quelque 4200 durant l'exercice précédent).

Le Préposé a participé à une cinquantaine d'événements, soit un peu plus que durant la période précédente. Il s'est notamment exprimé lors d'une conférence publique organisée par l'Université de Lausanne dans le cadre de la Journée internationale de la protection des données, fin janvier 2022. Dans son allocution, il a souligné que les autorités de protection des données œuvrent pour que la transformation numérique puisse se dérouler dans le respect du droit fondamental à la vie privée et à l'autodétermination.

Rapport d'activité et développement d'un nouveau site Internet

À la fin de l'année sous revue, le secteur Communication est composé de 3 personnes pour un total de 2,6 équivalents plein temps. Le travail avec les médias est une priorité, tout comme le projet de rapport d'activités annuel. La publication du 28e rapport d'activités 2020/2021, prescrite par l'art. 30 LPD, a eu lieu le 29 juin 2021. Le document, produit et imprimé en quatre langues, peut être consulté sur notre site Internet en version électronique ou en PDF accessible.

À l'automne 2021, le PFPDT a lancé le projet de refonte de son site Internet. Au terme d'une procédure d'appel d'offres, la phase de conception a été entamée dès 2022, en collaboration avec une agence externe. L'objectif est de simplifier la structure actuelle, complexifiée au fil des ans, et de mettre à jour les contenus afin que les utilisatrices et utilisateurs puissent disposer d'un site moderne, ergonomique et adapté à leurs besoins. Le nouveau site Internet du PFPDT tiendra compte des dispositions de la nouvelle loi sur la protection des données et sera mis en ligne avant l'entrée en vigueur de celle-ci.

Avis et recommandations

Au cours de l'année sous revue, le Préposé a publié divers avis et prises de positions sur des projets et événements actuels, notamment :

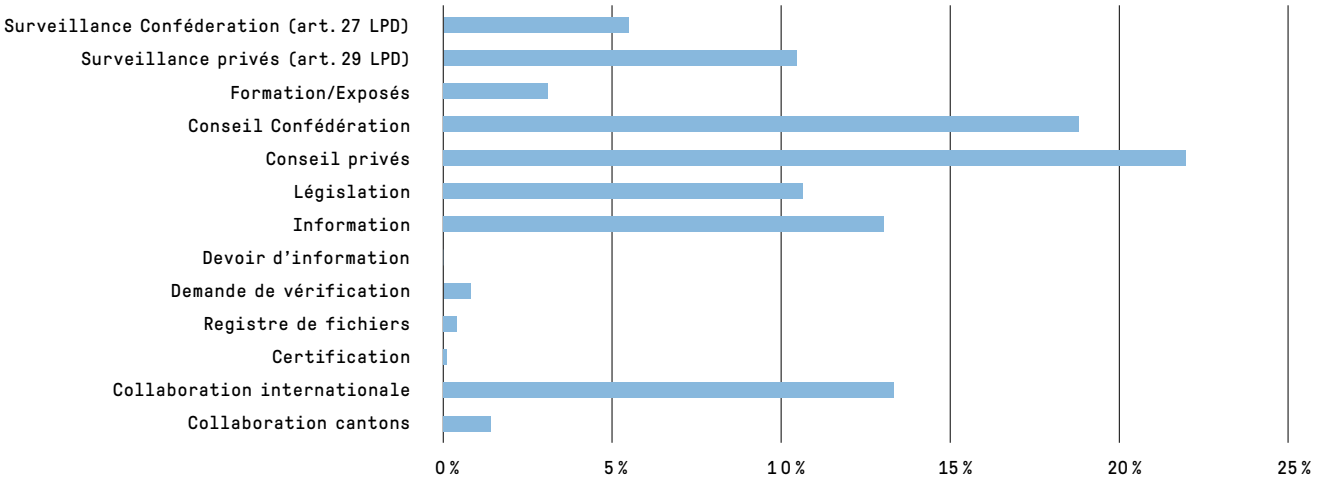
- établissements des faits concernant l'application SocialPass ainsi que les plateformes mesvaccins.ch et Swisstransplant
- surveillances présumées et non autorisées de personnes (Mitto AG)
- accompagnement du développement du certificat COVID et de la version light contenant un minimum de données
- transferts de données vers l'étranger
- transfert de données non conforme à la LPD, par la Fédération suisse de tir
- diverses fuites de données, notamment sur les réseaux sociaux

Nous avons en outre publié sur notre site 45 recommandations relatives à l'accès aux documents administratifs en vertu du principe de transparence (contre 26 en 2020).

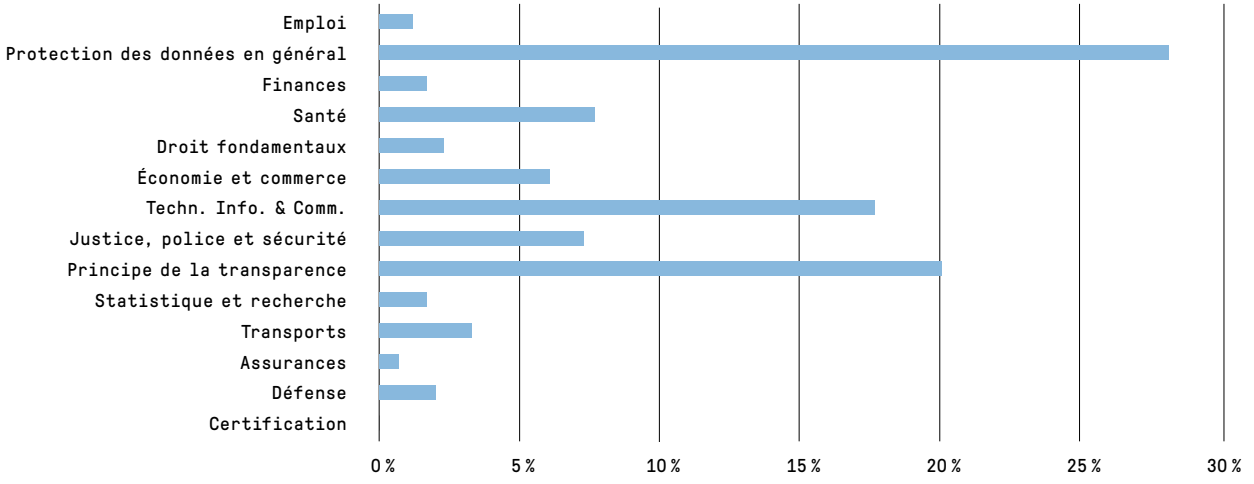
3.3 Statistiques

Statistiques des activités du PFPDT du 1er avril 2021 au 31 mars 2022 (Protection des données)

Charge de travail par tâche

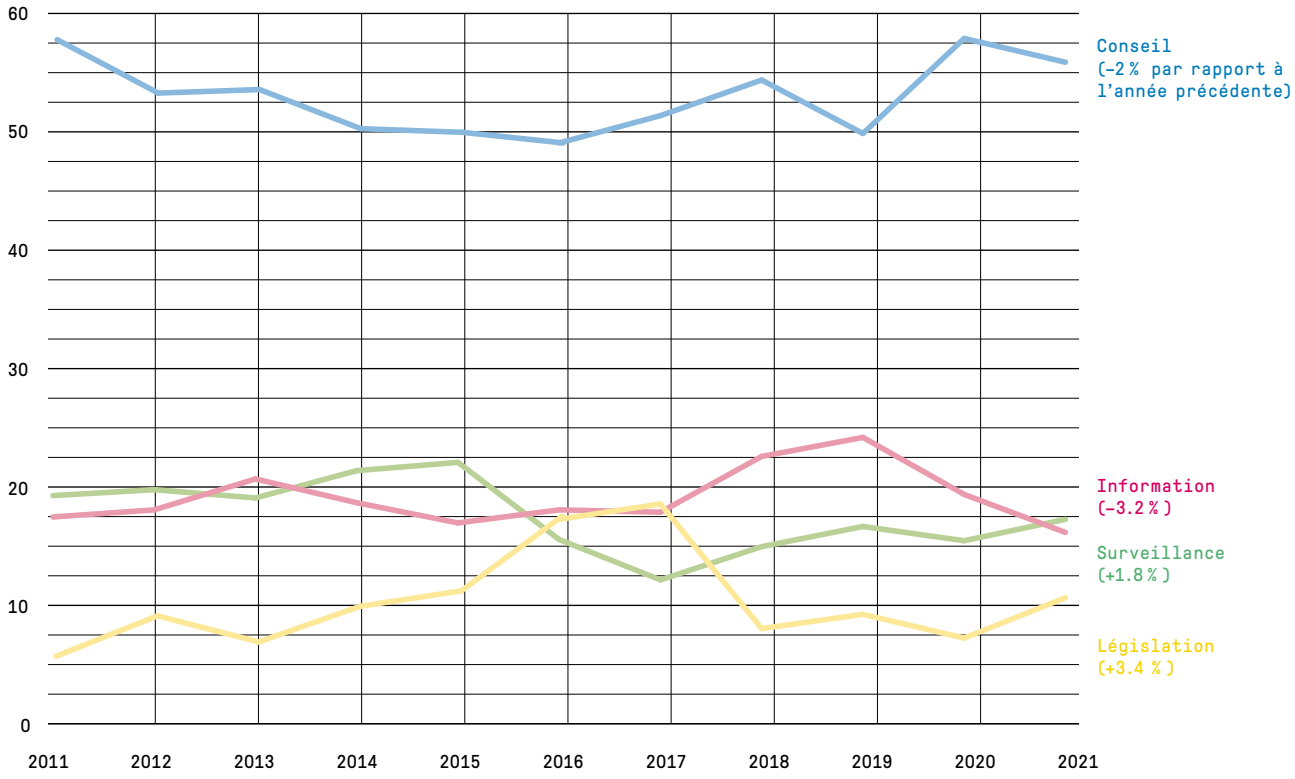


Charge de travail par domaine



Comparaison pluriannuelle

(en pourcentage)



Vue d'ensemble des demandes d'accès du 1er janvier au 31 décembre 2021

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	57	26	8	9	2	5	7
DFAE	156	77	15	47	2	5	10
DFI	422	168	25	139	21	38	31
DFJP	103	46	18	13	1	2	23
DDPS	281	203	11	38	7	3	19
DFF	119	54	22	21	6	9	7
DEFR	92	48	13	22	2	6	1
DETEC	146	71	10	35	6	10	14
MPC	8	0	4	0	1	0	3
SP	1	1	0	0	0	0	0
Total 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (3)	78 (7)	115 (8)
Total 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Total 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Total 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Total 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	–
Total 2016 (%)	558 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	–
Total 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	–
Total 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	–
Total 2013 (%)	461 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	–
Total 2012 (%)	522 (100)	230 (44)	140 (27)	123 (24)	19 (4)	6 (1)	–
Total 2011 (%)	481 (100)	206 (44)	127 (27)	128 (27)	0 (0)	9 (2)	–

Statistique des demandes d'accès selon la loi sur la transparence du 1er janvier au 31 décembre 2021 (en pourcentage)

	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	**41**	19	6	7	2	0	7
	PFPDT	**16**	7	2	2	0	5	0
	Total	**57**	**26**	**8**	**9**	**2**	**5**	**7**
Département fédéral des affaires étrangères DFAE	DFAE	**156**	77	15	47	2	5	10
	Total	**156**	**77**	**15**	**47**	**2**	**5**	**10**
Département fédéral de l'intérieur DFI	SG DFI	**13**	8	0	2	0	2	1
	BFEG	**24**	20	0	0	1	0	3
	OFC	**1**	0	1	0	0	0	0
	AFS	**1**	1	0	0	0	0	0
	MétéoSuisse	**0**	0	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	OFSP	**251**	90	11	101	6	27	16
	OFS	**12**	8	3	0	0	0	1
	OFAS	**13**	8	3	1	0	0	1
	compenswiss	**2**	1	1	0	0	0	0
	OSAV	**28**	17	1	9	1	0	0
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**72**	15	3	26	11	8	9
	SUVA	**5**	0	2	0	2	1	0
	Total	**422**	**168**	**25**	**139**	**21**	**38**	**31**
Département fédéral de justice et police DFJP	SG DFJP	**14**	7	0	1	0	1	5
	OFJ	**38**	13	10	0	0	0	15
	fedpol	**14**	10	3	1	0	0	0
	METAS	**1**	1	0	0	0	0	0
	SEM	**24**	10	2	9	1	0	2
	Service SCPT	**3**	0	0	2	0	0	1
	ISDC	**5**	2	3	0	0	0	0
	IPI	**2**	2	0	0	0	0	0
	CFMJ	**0**	0	0	0	0	0	0
	CAF	**1**	1	0	0	0	0	0
	ASR	**0**	0	0	0	0	0	0
	CSI	**0**	0	0	0	0	0	0
	CNPT	**1**	0	0	0	0	1	0
	Total	**103**	**46**	**18**	**13**	**1**	**2**	**23**

	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	**27**	10	0	8	0	1	8
	Défense	**29**	17	1	7	3	1	0
	SRC	**28**	0	6	15	0	0	7
	armasuisse	**12**	3	4	3	0	1	1
	OFSPO	**172**	170	0	0	2	0	0
	OFPP	**8**	1	0	5	0	0	2
	swisstopo	**5**	2	0	0	2	0	1
	OAC	**0**	0	0	0	0	0	0
	Total	**281**	**203**	**11**	**38**	**7**	**3**	**19**
Département fédéral des finances DFF	SG DFF	**25**	8	6	7	0	2	2
	UPIC [1]	**0**	0	0	0	0	0	0
	AFF	**7**	2	0	3	0	0	2
	OFPER	**4**	4	0	0	0	0	0
	AFC	**14**	4	7	3	0	0	0
	ARD [2]	**42**	22	3	7	4	6	0
	OFCL	**5**	3	1	0	1	0	0
	OFIT	**7**	5	0	0	1	0	1
	CDF	**9**	1	4	1	0	1	2
	SFI	**3**	3	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	DdC	**3**	2	1	0	0	0	0
	Total	**119**	**54**	**22**	**21**	**6**	**9**	**7**

[1] **depuis le 1.1.2021 ChF TNI**

[2] **Depuis le 1.1.2022 OFDF**

	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'économie, de la formation et de la recherche DEFR	SG DEFR	**6**	6	0	0	0	0	0
	SECO	**28**	18	3	4	2	1	0
	SEFRI	**13**	10	2	0	0	0	1
	OFAG	**13**	3	1	8	0	1	0
	Agroscope	**3**	2	0	1	0	0	0
	OFAE	**2**	1	1	0	0	0	0
	OFL	**1**	0	0	1	0	0	0
	SPR	**4**	1	3	0	0	0	0
	COMCO	**10**	4	1	3	0	2	0
	CIVI	**0**	0	0	0	0	0	0
	BFC	**1**	0	0	0	0	1	0
	FNS	**0**	0	0	0	0	0	0
	IFFP	**1**	0	1	0	0	0	0
	Conseil EPF	**9**	2	1	5	0	1	0
	Innosuisse	**1**	1	0	0	0	0	0
	Total	**92**	**48**	**13**	**22**	**2**	**6**	**1**
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	**12**	8	1	0	0	1	2
	OFT	**7**	3	0	2	0	1	1
	OFAC	**10**	6	1	1	1	1	0
	OFEN	**11**	3	3	3	0	1	1
	OFROU	**6**	5	0	1	0	0	0
	OFCOM	**23**	9	0	11	0	1	2
	OFEV	**64**	34	4	15	3	1	7
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	IFSN	**9**	2	0	1	2	3	1
	PostCom	**3**	1	0	1	0	1	0
	AIEP	**1**	0	1	0	0	0	0
	Total	**146**	**71**	**10**	**35**	**6**	**10**	**14**
Ministère public de la Confédération MPC	MPC	**8**	0	4	0	1	0	3
	Total	**8**	**0**	**4**	**0**	**1**	**0**	**3**
Services du Parlament SP	SP	**1**	1	0	0	0	0	0
	Total	**1**	**1**	**0**	**0**	**0**	**0**	**0**
	Somme totale	**1385**	**694**	**126**	**324**	**48**	**78**	**115**

Demandes d'accès 2021 liées au Corona

	Section concernée	Demandes liées au 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	**5**	3	1	1	0	0	0
	PFPDT	**0**	0	0	0	0	0	0
	Total	**5**	**3**	**1**	**1**	**0**	**0**	**0**
Département fédéral des affaires étrangères DFAE	DFAE	0	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Département fédéral de l'intérieur DFI	SG DFI	**6**	5	0	0	0	1	0
	BFEG	**0**	0	0	0	0	0	0
	OFC	**0**	0	0	0	0	0	0
	AFS	**0**	0	0	0	0	0	0
	MétéoSuisse	**0**	0	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	OFSP	**217**	82	2	93	4	20	16
	OFS	**0**	0	0	0	0	0	0
	OFAS	**1**	1	0	0	0	0	0
	compenswiss	**0**	0	0	0	0	0	0
	OSAV	**0**	0	0	0	0	0	0
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**41**	6	2	17	6	6	4
	SUVA	**1**	0	0	0	1	0	0
	Total	**266**	**94**	**4**	**110**	**11**	**27**	**20**
Département fédéral des finances DFF	SG DFF	**5**	0	4	1	0	0	0
	UPIC [1]	**0**	0	0	0	0	0	0
	AFF	**6**	1	0	3	0	0	2
	OFPER	**0**	0	0	0	0	0	0
	AFC	**1**	0	1	0	0	0	0
	ARD [2]	**2**	0	0	2	0	0	0
	OFCL	**1**	0	0	0	1	0	0
	OFIT	**6**	3	0	1	1	0	1
	CDF	**1**	0	0	0	0	1	0
	SFI	**0**	0	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	DdC	**0**	0	0	0	0	0	0
	Total	**22**	**4**	**5**	**7**	**2**	**1**	**3**

[1] depuis le 1.1.2021 ChF TNI

[2] Depuis le 1.1.2022 OFDF

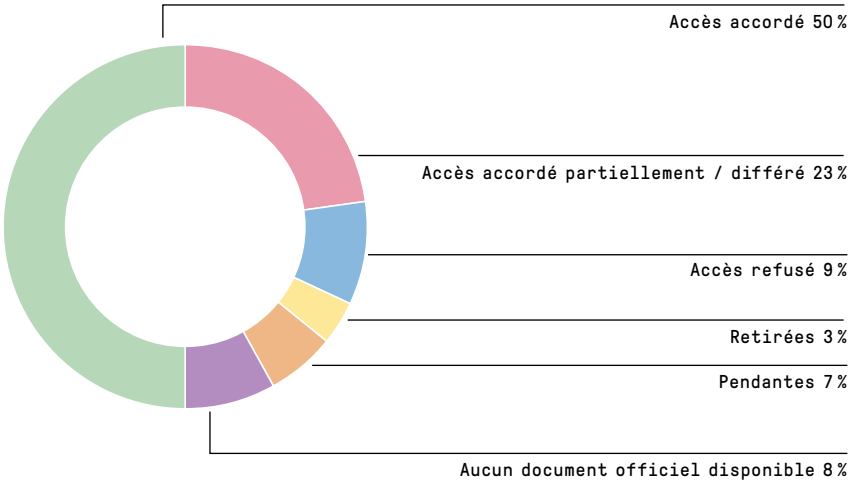
	Section concernée	Demandes liées au Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de justice et police DFJP	SG DFJP	**1**	1	0	0	0	0	0
	OFJ	**0**	0	0	0	0	0	0
	fedpol	**0**	0	0	0	0	0	0
	METAS	**0**	0	0	0	0	0	0
	SEM	**0**	0	0	0	0	0	0
	Service SCPT	**0**	0	0	0	0	0	0
	ISDC	**0**	0	0	0	0	0	0
	IPI	**0**	0	0	0	0	0	0
	CFMJ	**0**	0	0	0	0	0	0
	CAF	**0**	0	0	0	0	0	0
	ASR	**0**	0	0	0	0	0	0
	CSI	**0**	0	0	0	0	0	0
	CNPT	**0**	0	0	0	0	0	0
	Total	**1**	**1**	**0**	**0**	**0**	**0**	**0**
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	**0**	0	0	0	0	0	0
	OFT	**0**	0	0	0	0	0	0
	OFAC	**1**	0	0	1	0	0	0
	OFEN	**0**	0	0	0	0	0	0
	OFROU	**0**	0	0	0	0	0	0
	OFCOM	**1**	0	0	1	0	0	0
	OFEV	**0**	0	0	0	0	0	0
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	IFSN	**0**	0	0	0	0	0	0
	PostCom	**0**	0	0	0	0	0	0
	AIEP	**0**	0	0	0	0	0	0
	Total	**2**	**0**	**0**	**2**	**0**	**0**	**0**
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	**0**	0	0	0	0	0	0
	Défense/armée	**25**	15	1	5	3	1	0
	SRC	**0**	0	0	0	0	0	0
	armasuisse	**0**	0	0	0	0	0	0
	OFSPO	**4**	2	0	0	2	0	0
	OFPP	**1**	0	0	1	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OAC	**0**	0	0	0	0	0	0
	Total	**30**	**17**	**1**	**6**	**5**	**1**	**0**

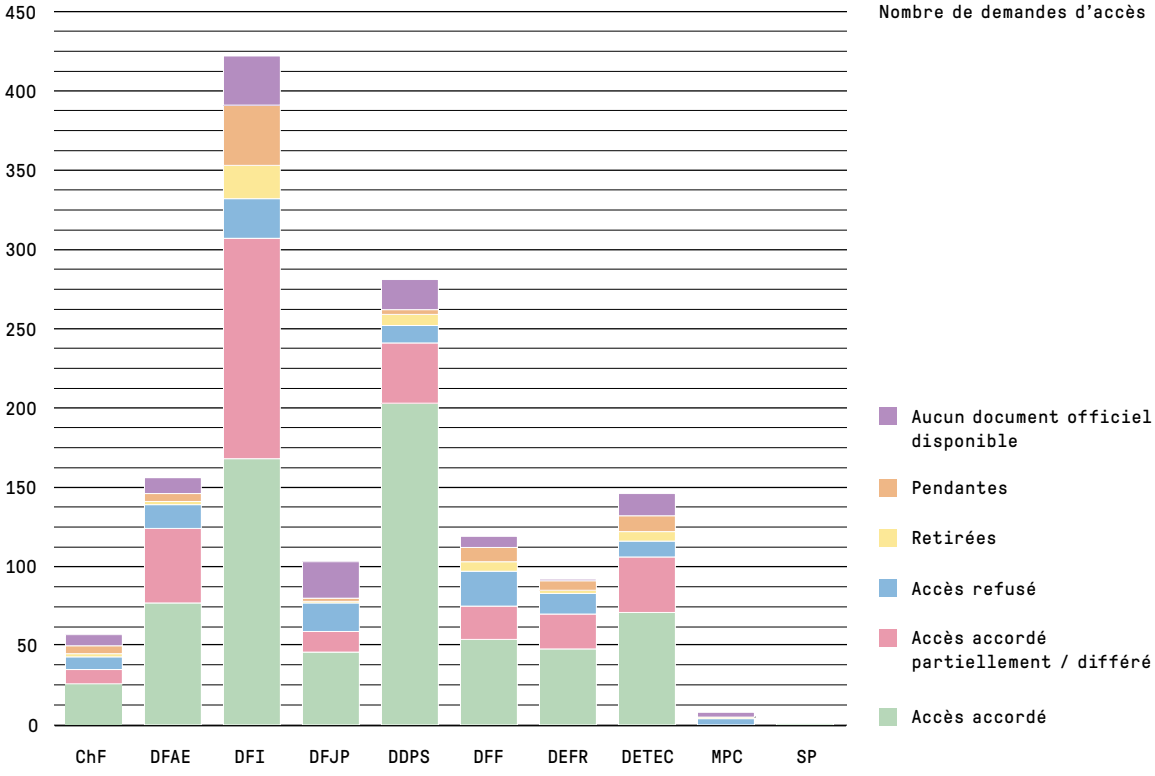
	Section concernée	Demandes liées au Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de l'économie, de la formation et de la recherche DEFR	SG DEFR	**1**	1	0	0	0	0	0
	SECO	**5**	1	1	3	0	0	0
	SEFRI	**1**	0	0	0	0	0	1
	OFAG	**0**	0	0	0	0	0	0
	Agroscope	**0**	0	0	0	0	0	0
	OFAE	**0**	0	0	0	0	0	0
	OFL	**0**	0	0	0	0	0	0
	SPR	**0**	0	0	0	0	0	0
	COMCO	**0**	0	0	0	0	0	0
	CIVI	**0**	0	0	0	0	0	0
	BFC	**0**	0	0	0	0	0	0
	FNS	**0**	0	0	0	0	0	0
	IFFP	**0**	0	0	0	0	0	0
	Conseil EPF	**3**	0	1	2	0	0	0
	Innosuisse	**0**	0	0	0	0	0	0
	Total	**10**	**2**	**2**	**5**	**0**	**0**	**1**
Ministère public de la Confédération MPC	MPC	**0**	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Services du Parlament SP	SP	**0**	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	Somme totale	**336**	**121**	**13**	**131**	**18**	**29**	**24**

Nombre de demandes en médiation

Catégories de requérants	2021	2020	2019	2018	2017
Médias	53	31	34	24	21
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	49	42	40	26	35
Représentants de milieux intéressés (associations,organisations, sociétés, etc.)	16	5	7	9	14
Avocats	12	7	5	4	2
Entreprises	19	7	47	13	7
Universités	0	1			
Total	**149**	**93**	**133**	**76**	**79**

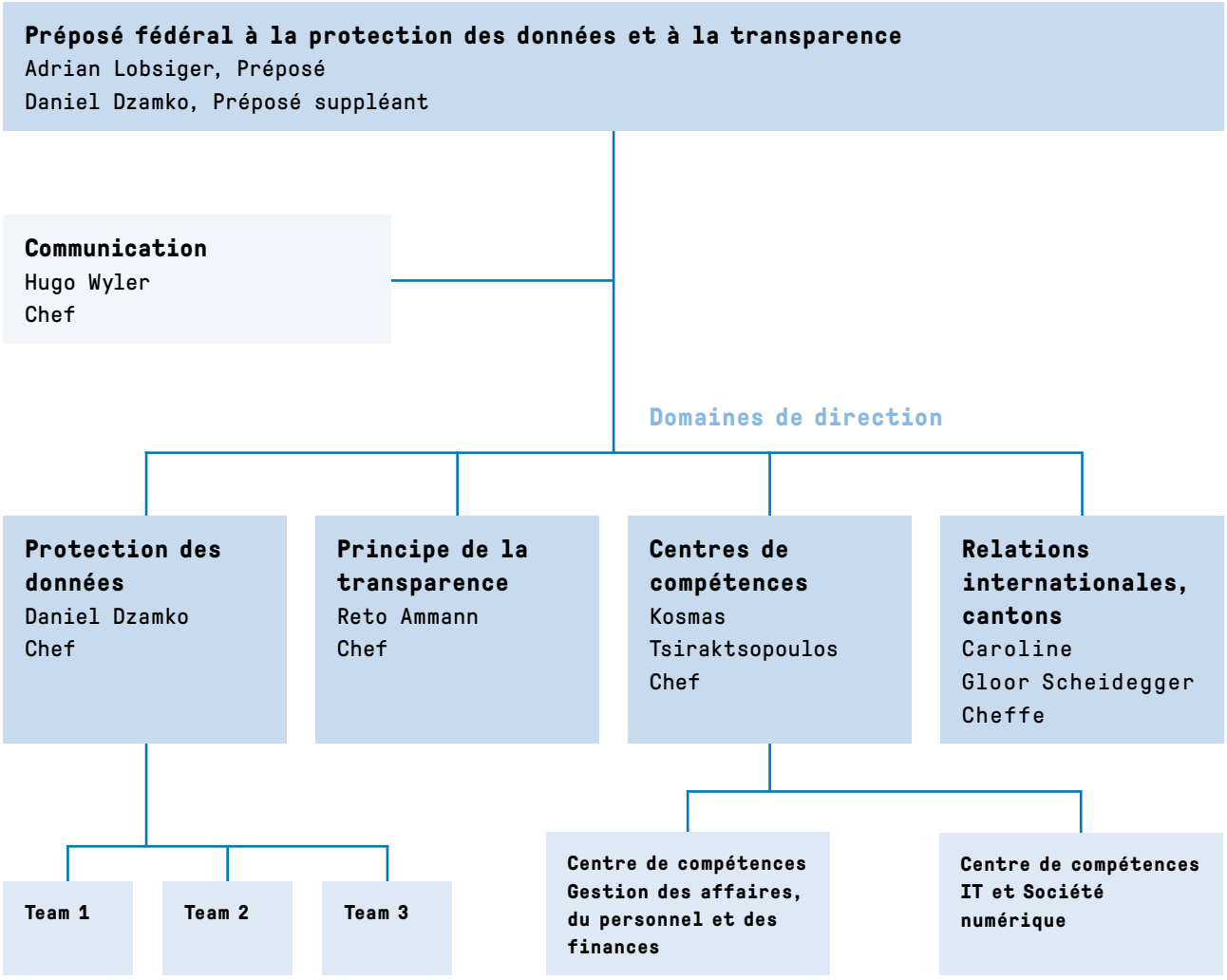
Traitement des demandes d'accès du 1er janvier au 31 décembre 2021





3.4 Organisation du PFPDT (État au 31 mars 2021)

Organigramme



Personnel du PFPDT

Nombre d'employés	39		
EPT	32.4		
par sexe	Femmes	19	49 %
	Hommes	20	51 %
par pourcentage d'emploi	1–89 %	27	69 %
	90–100 %	12	31 %
par langue	Allemand	29	77 %
	Français	8	20 %
	Italien	1	3 %
par âge	20–49 ans	23	59 %
	50–65 ans	16	41 %
Postes dirigeants	Femmes	3	33 %
	Hommes	6	67 %

Liste des abréviations

AIPD Analyse d'impact relative à la protection des données

AMVP Assemblée mondiale pour la protection de la vie privée

CCT Clauses contractuelles types

CDM Centre des données sur la mobilité

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

DaziT Programme de transformation globale de l'OFDF

DEP Dossier électronique du patient

e-ID Identité électronique

Fedpol Office fédéral de la police

IA Intelligence artificielle

IKO Centre de renseignements sur le crédit à la consommation

LDEP Loi fédérale sur le dossier électronique du patient

LDP Loi fédérale sur les droits politiques

LIDMo Loi fédérale concernant l'infrastructure de données sur la mobilité

LMETA Loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités

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 sur les services d'identification électronique (loi 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

NADIM Infrastructure nationale de données pour la mobilité

NCSC Centre national pour la cybersécurité

nLPD Nouvelle loi sur la protection des données

OCDE Organisation de coopération et de développement économiques

OCPD Ordonnance sur les certifications en matière de protection des données

OFDF Office fédéral de la douane et de la sécurité des frontières

OLPD Ordonnance relative à la loi fédérale sur la protection des données

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

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

nLPD Loi révisée sur la protection des données

RGPD Règlement général sur la protection des données

SAS Service d'accréditation suisse

SEC Autorité américaine de surveillance des marchés financiers

SRC Service de renseignement de la Confédération

TIC Technologies de l'information et de la communication

TNI Secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale

ZEK Centrale d'information de crédit

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. 410.029.F

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

Chiffres clés

Dépenses de protection des données

55,8 %	17,3 %	16,2 %	10,7 %
Conseils	Surveillance	Information	Législation

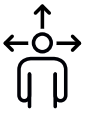
Demandes d'accès Principe de la transparence (LTrans)

50 %	23 %	9 %	4 %	6 %	8 %
accordé	accordé partiellement/ differé	refusé	retirées	pendantes	aucun document officiel disponible

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

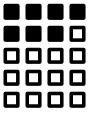
Les personnes concernées donnent leur consentement et jouissent d'une réelle liberté de choix.

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.

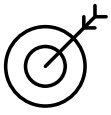
Exactitude des données

Le traitement s'effectue avec des données correctes.



Proportionnalité

Pas de collecte systématique 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, 10h–12h)
Téléfax : +41 (0)58 465 99 96