27e Rapport d'activités 2019/20

Préposé fédéral à la protection des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2019/2020
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 2019 au 31 mars 2020.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra


We'll
show
you
the
way

Avant-propos

Ce ne sont plus les virus informatiques mais les virus naturels qui font la une des journaux à la fin de cette période sous revue. Le coronavirus pénètre dans les tissus vivants des êtres humains, révélant notre vulnérabilité en tant qu'êtres biologiques viscéralement effrayés par une menace invisible.

Notre société numérisée offre une multitude de services susceptibles de nous protéger face au monde invisible des virus et des germes, apaisant ainsi nos peurs. Contre les virus informatiques nous avons les pare-feux numériques. Contre la contamination par les germes, le télétravail, en ces jours, est d'un précieux secours. Et les applications qui, par l'analyse des données de mobilité, créent des conditions de voyage plus confortables en permettant de respecter une distance minimale, contribuent à protéger notre santé de manière préventive.

Malgré les avantages évidents des technologies numériques, malgré l'accent légitime mis sur le civisme, la discipline et la solidarité de crise, et malgré notre peur naturelle de ce virus invisible, nous ne devrions pas pour autant abandonner notre autonomie de pensée. C'est précisément en ces temps de pandémie et de crise économique que nous devons rester vigilants et éviter que les théories du complot, la superstition ou la froide soif de pouvoir ne prennent le dessus et ne nous poussent dans les griffes de la tutelle numérique.

Nul ne peut dire, au moment de l'impression du présent rapport, quand nous retournerons à la normalité. Nous espérons tous que cela sera pour bientôt, avec le moins de victimes possible. J'associe également à cet espoir que «le jour d'après », nous retrouvions notre autodétermination informationnelle intacte et que l'argent liquide, anonyme par essence, survivra à cette crise même s'il peut être porteur de germes.

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

Berne, le 31 mars 2020

Protection des données

Principe de la transparence

Le PFPDT

Défis actuels

I Numérisation

La crise provoquée par le nouveau coronavirus et le passage obligé au télétravail, ainsi que les achats en ligne, montrent bien la place qu'Internet et les technologies de l'information et de la communication ont pris dans la vie quotidienne de la population suisse.

Technologie et économie

Au cours de la période sous revue, le Préposé a constaté avec inquiétude que de plus en plus de privés pratiquent désormais le traitement automatisé de grandes quantités de données biométriques. Ainsi certaines sociétés privées se procurent ce type de données par un contact direct avec leurs clients, par exemple lorsque ces derniers s'identifient par leur voix (cf. ch. 1.4) ; d'autres obtiennent d'importantes quantités de données biométriques sur Internet, par exemple en récupérant des images faciales disponibles sur les réseaux sociaux, puis en traitant les images copiées avec un logiciel de reconnaissance faciale et les enrichissent avec d'autres données personnelles (cf. ch. 1.1). Alors que dans les États autoritaires, les services en charge de la sécurité peuvent accéder à leur gré aux données personnelles, soit directement, soit par l'intermédiaire des opérateurs de services et de plateformes de télécommunication, des limites sont posées aux autorités de police des démocraties occidentales, limites pouvant toutefois être aménagées de manière très différente : alors qu'aux États-Unis par exemple, certaines autorités de sécurité utilisent déjà des services payants de reconnaissance faciale appartenant à des sociétés privées, en Suisse les programmes automatisés de reconnaissance faciale des autorités de police devraient se fonder sur des bases légales ; or celles-ci ne sont actuellement fournies ni par le législateur fédéral, ni par les législateurs cantonaux.

La tendance croissante de certains États à exploiter le potentiel accru du numérique afin de surveiller la population s'est déjà traduite par des demandes d'échange d'images, également dans le cadre de la coopération policière européenne prévue par la Convention de Prüm (cf. ch. 1.9). Le Préposé estime que tôt ou tard, les organes de police fédéraux et cantonaux requerront aussi des autorités politiques la création de lois leur permettant une large utilisation de la technologie de reconnaissance faciale. À ses yeux, ces lois seraient problématiques. Elles menaceraient de transformer en exception la règle actuelle selon laquelle tout un chacun se déplace librement et anonymement dans l'espace public, même si d'aucuns soutiendraient que les comparaisons automatiques et les analyses de données faciales seraient limitées aux infractions particulièrement graves. L'expérience montre que les seuils de criminalité en droit pénal sont progressivement abaissés et assouplis à des fins étrangères aux objectifs initialement fixés en matière de sécurité, de police des étrangers et administrative, une fois en place la législation requise.

Un autre motif de préoccupation est le nombre alarmant de plaintes concernant la perte de données de santé, de dossiers du personnel, de demandes de crédit, de photographies, de communications par chat et par e-mail qui ont été déposées au cours de la période sous revue. Les fuites injustifiées de données personnelles et la diffusion de données volées augmentent la multitude de données personnelles accessibles sur Internet et portent irrémédiablement atteinte à la sphère privée. Les exploitants de grands services de cloud, qui détiennent également des quantités astronomiques de données d'images privées, portent une grande responsabilité : celle d'assurer la sécurité de ces données par des moyens techniques et organisationnels appropriés.

Société et politique des données

Dans le cadre de la lutte mondiale contre le coronavirus, les gouvernements des régions asiatiques gravement touchées et dans lesquelles la pandémie s'est déclarée ont encore étendu leurs moyens de surveillance numérique de la population, déjà très invasifs selon les normes occidentales, pour éviter toute propagation du virus. Confronté à une extension de la contagion en Suisse, le Conseil fédéral a lui aussi ordonné des mesures sanitaires et, après avoir décrété le 16 mars 2020 l'état de situation extraordinaire au sens de l'art. 7 de la loi sur les épidémies, il a alors ordonné des mesures non décrites précisément dans cette loi. Celle-ci exige seulement que les mesures soient nécessaires. Dans ses prises de position publiques sur la pandémie, actualisées en permanence, le Préposé n'a eu de cesse de souligner que le recours aux technologies numériques pour la collecte et l'analyse de données de mobilité et de proximité doit s'avérer proportionnée à l'objectif de prévention de la contamination, c'est-à-dire qu'elles doivent être pertinentes d'un point de vue épidémiologique et aptes à avoir un effet justifiant une atteinte à la personnalité des individus concernés afin de contenir la pandémie, en tenant compte du stade concret de celle-ci. Le 24 mars 2020, le Préposé a créé le groupe de travail interne « Task Force Corona » ; il a depuis examiné divers projets privés et publics de lutte numérique contre la pandémie. Par ailleurs, sur son site Internet, le Préposé informe en continu sur les travaux de la Task Force et leurs résultats (www.leprepose.ch).

Pour le Préposé, cet événement collectif tragique qu'est la pandémie due au coronavirus ne doit pas se traduire par une atteinte permanente à l'autodétermination informationnelle et à la sphère privée de la population suisse. Dans sa prise de position, il a souligné à titre préventif, en ce qui concerne les traitements de données personnelles dans le cadre de la lutte contre le virus, que les données récoltées devront être effacées ou anonymisées lorsque la menace de pandémie aura cessé.

« La gestion de la pandémie ne doit pas entraîner une atteinte permanente à la liberté et à l'autonomie. »

Législation

Les travaux législatifs concernant la révision totale de la loi fédérale sur la protection des données sont déjà bien avancés. Le projet ayant été discuté par les deux Chambres, l'élimination des divergences n'a pas encore eu lieu à la fin de la période sous revue, des retards étant de surcroît d'ores et déjà à déplorer en raison de la pandémie. Le Préposé espère que malgré l'épidémie de COVID-19, ces divergences seront bientôt éliminées et que le vote final pourra avoir lieu à la session d'été.

II Activité de conseil et surveillance

En tant qu'autorité de surveillance, le Préposé doit veiller à ce qu'indépendamment des possibilités techniques, les traitements de données personnelles soient conformes 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 leur phase de planification et d'élaboration et qu'ils les documentent à l'égard du collaborateur compétent dans leur entreprise et des autorités de protection des données. Dans ce contexte, nous avons poursuivi au cours de l'année sous revue l'accompagnement de nombreux projets impliquant des mégadonnées, tant auprès d'autorités fédérales que d'entreprises privées.

Dans la perspective de projets à grande échelle comportant des risques élevés en matière de protection des données et dans le but d'utiliser efficacement ses propres ressources, le Préposé continue à encourager l'utilisation responsable d'instruments de travail modernes tels que l'analyse d'impact en matière de protection des données et, le cas échéant, la création d'organes de protection des données au sein des entreprises. Aussi la part de ses dépenses totales consacrée à l'accompagnement de projets du secteur privé a-t-elle légèrement diminué au cours de l'année sous revue.

Dans la perspective des élections fédérales de l'automne 2019, le Préposé a mis tout particulièrement l'accent sur ses activités de conseil ; ainsi, en décembre 2018, il a publié en collaboration avec les autorités cantonales de protection des données, un guide sur la protection des données dans le contexte des élections et des votations (www.edoeb.admin.ch/elections).

Dans la phase finale de la campagne électorale, le Préposé a encouragé les partis politiques à améliorer leurs sites Internet à l'aide de son guide relatif aux élections et votations publié en collaboration avec les autorités cantonales de protection des données et la mise à disposition d'une liste de contrôle pour vérifier la conformité des sites Internet à la protection des données, qui a reçu beaucoup d'attention de la part des médias.

Un autre point fort a été l'accompagnement du secteur des transports dans l'élaboration d'applications de billetterie électronique (cf. ch. 1.8). Le traitement des données relatives à la mobilité s'avère tout particulièrement délicat car il conduit facilement à des profils de personnalité qui ne peuvent être pseudonymisés, voire anonymisés, qu'au prix de grands efforts (cf. ch. 1.8). Dans ce contexte, il convient de se féliciter que le Conseil des États ait reconnu que la protection spéciale contre les traitements permettant d'établir des profils (protection qui disparaîtra avec la révision de la LPD) doit être maintenue et ancrée sous la nouvelle dénomination de « profilage ». Il est à espérer que les Chambres fédérales s'entendront pour que le niveau de protection de la LPD actuelle puisse au moins être maintenu (cf. Accent I).

Après leur nette réduction au cours de la période 2015/16, le Préposé a été à nouveau en mesure d'augmenter les dépenses affectées à ses tâches de surveillance au cours de la période sous revue et de la période antérieure. Toutefois, elles demeurent inférieures à la moyenne enregistrée sur les périodes précédentes. Compte tenu de la faiblesse persistante des moyens financiers dont dispose l'autorité, cette augmentation n'a été obtenue que par la réduction d'autres prestations. Durant la période sous revue, le Préposé n'a pas été à même de répondre dans la mesure souhaitée aux attentes justifiées du public en ce qui concerne les mesures de surveillance applicables aux traitements de données personnelles opérés par les applications de consommateurs et sur les réseaux sociaux (cf. ch. 3.1).

Dans le cadre de l'accompagnement des grands projets numériques, la protection des données en entreprise peut établir une passerelle importante avec la protection des données assurée par les autorités; le Préposé et son suppléant ont donc entretenu régulièrement des contacts avec les associations de conseillers à la protection des données des entreprises privées de Suisse alémanique et de Suisse romande au cours de la période sous revue. Ces rencontres ont été très suivies et se sont avérées très utiles pour toutes les parties concernées.

« La protection des données en entreprise constitue une passerelle importante vers la protection des données assurée par les autorités dans le cadre de l'accompagnement de grands projets numériques. »

III Coopération nationale et internationale

Coopération nationale

Le Préposé a encore intensifié sa collaboration avec les autorités cantonales de protection des données. Citons quelques exemples : discussions techniques avec les préposés cantonaux à la protection des données en vue de l'introduction du dossier électronique du patient (cf. ch. 1.5), communication conjointe entre les autorités fédérales et cantonales de protection des données à l'occasion de la Journée internationale de la protection des données en matière de dangers pour la sphère privée dans les transports privés et publics (cf. ch. 3.2), participation aux différentes séances du Bureau et assemblées générales de la Conférence des Préposé(e)s suisses à la protection des données (Privatim) et aux réunions des préposés latins à la protection des données. Ces rencontres ont permis de multiples échanges à propos des procédures de consultation en cours et des expériences dans les différentes compétences en matière de conseil et de contrôle.

Signature de la Convention 108+

Conformément à la décision du Conseil fédéral, la Suisse a officiellement signé la Convention 108+ le 21 novembre 2019 à Strasbourg. Le message relatif à l'approbation du protocole a été adopté par le Conseil fédéral à l'intention du Parlement le 6 décembre 2019. L'adhésion à ce nouvel instrument permettra à la Suisse de garantir un niveau élevé de protection des données dans la sphère privée et simplifiera la transmission transfrontière de données dans les secteurs public et privé. Elle est également un élément important dans la perspective de la prochaine évaluation de la Commission européenne (cf. infra).

Nouveau droit européen de la protection des données

Le Règlement général de l'Union européenne sur la protection des données (RGPD) est entré en vigueur en mai 2018. Le Préposé suit de près son application dans les différents pays européens et met régulièrement à jour les feuillets thématiques destinés aux entreprises suisses dont la première version remonte à l'automne 2017. Nous entendons continuer à soutenir ces entreprises tant par nos conseils que par nos actions.

« Le travail et la consommation se délocalisent au domicile, en faveur du télétravail et des achats en ligne. »

Évaluation du niveau de protection des données

La Commission européenne évalue le niveau de protection des données dans les pays tiers et a attesté pour la dernière fois en 2000 que la Suisse dispose d'un niveau de protection des données adéquat. Les entreprises de l'UE peuvent donc échanger des données personnelles avec des entreprises sises en Suisse sans autre démarche. Le processus d'évaluation de l'UE sur la base du RGPD a officiellement débuté en mars 2019. Au cours de l'année sous revue, le Préposé a soutenu par son savoir-faire le groupe de travail dirigé par l'Office fédéral de la justice (cf. ch. 1.9). Le rapport de la Commission est attendu pour la fin mai 2020.

À la suite du référendum britannique de juin 2016 sur le retrait de l'Union européenne (Brexit), le Royaume-Uni a quitté l'UE le 1er février 2020. Notre autorité a participé à de nombreuses réunions avec les autorités fédérales et les autorités britanniques afin de garantir que la libre circulation des données personnelles entre la Suisse et le Royaume-Uni soit également possible après le Brexit. Le Royaume-Uni est considéré comme un pays disposant d'un niveau de protection adéquat et le Préposé ne voit actuellement aucune raison de modifier son statut. L'UE décidera d'ici la fin de l'année 2020 si elle reconnaît l'adéquation de la législation sur la protection des données du Royaume-Uni. Le Préposé suit ces développements avec attention (cf. ch. 1.9).

Swiss-US Privacy Shield

À l'automne 2019, nous avons effectué le second examen de surveillance du bouclier de protection des données entre la Suisse et les États-Unis (Swiss-US Privacy Shield) dans le cadre d'une délégation dirigée par le Seco. Si ce contrôle a de nouveau mis en évidence certaines faiblesses, le fonctionnement de cet instrument de protection a été toutefois encore amélioré (cf. ch. 1.9).

Un arrêt très attendu est toujours en suspens, celui sur l'affaire actuellement traitée par la Cour de justice de l'Union européenne (CJUE) concernant le transfert de données de l'UE vers les États-Unis (Schrems II) ; le cas échéant, cet arrêt sera aussi l'occasion d'évaluer l'accord-cadre UE-US Privacy Shield. Il n'aura pas de répercussions directes pour la Suisse. Mais une fois cet arrêt rendu, le Préposé en analysera l'impact éventuel sur l'accord-cadre Swiss-US Privacy Shield.

« Les entreprises de l'UE peuvent échanger des données personnelles avec des entreprises suisses sans prendre de mesures particulières. »

Protection des données

1.1 Numérisation et droits fondamentaux

Élections et votations : fonctionnalités de Facebook

À l'occasion des élections fédérales de 2019, Facebook a lancé, sur sa plateforme sociale, de nouvelles fonctionnalités à l'intention des électeurs suisses. L'entreprise a confirmé au Préposé son respect des exigences en matière de protection des données figurant dans le guide relatif aux élections et votations.

Ayant appris par les médias que Facebook envisageait avoir recours à différentes fonctionnalités, telles que les boutons de vote, en vue des élections fédérales de 2019, le Préposé s'est adressé par écrit aux contacts désignés par l'entreprise et les a invités à prendre position. Dans sa lettre, il a rappelé qu'en vertu de son guide relatif aux élections et votations (voir encadré), les opérateurs de réseaux sociaux sont également tenus d'informer les personnes concernées de manière juste et complète sur le traitement de leurs données et le fonctionnement des méthodes de traitement utilisées dans le contexte d'élections. Cette transparence est indispensable pour que les électeurs puissent évaluer l'impact de ces méthodes sur la formation de leur opinion ou sur leur comportement électoral.

Facebook Ireland Ltd. a confirmé par écrit au Préposé qu'il mettrait ces fonctionnalités en service le jour précédant les élections et le jour du scrutin. La plateforme sociale a également déclaré que le jour du scrutin, elle rappellerait la tenue des élections sans exception à tous les utilisateurs de Facebook en Suisse, âgés de 18 ans et plus. Facebook nous a également assuré qu'il ne ciblerait aucun groupe ou individu pour l'envoi de ce rappel. Selon les assurances écrites fournies par Facebook, le seul but de ces fonctionnalités était de sensibiliser les utilisateurs aux élections et d'encourager la participation électorale – par exemple en permettant aux personnes concernées de publier dans leur profil qu'elles ont effectivement voté. Facebook a souligné que dans ce contexte, il ne traiterait pas les opinions politiques des utilisateurs et a par ailleurs précisé qu'il s'engageait à respecter les exigences en matière de transparence formulées dans notre guide. Au moyen d'hyperliens, les personnes concernées pouvaient s'informer de manière approfondie sur les fonctionnalités, les méthodes et les bases de traitement. Le Préposé a informé le public des garanties données par Facebook sur son site Internet.

Après l'activation des fonctionnalités de vote, le Préposé a examiné la mise en œuvre des obligations de transparence et a constaté que Facebook informait comme indiqué les utilisateurs sur les traitements de données correspondants. Il a également constaté que toutes les autres activités, telles que les mentions de participation aux élections, ont été effectuées par les utilisateurs eux-mêmes et de manière volontaire. Faute de constater

Mise à jour du guide et nouvelle check-list pour les partis politiques

Avant la dernière étape des élections fédérales de 2019, le Préposé a invité les partis politiques à améliorer leurs sites Internet d'une part en mettant à jour le guide relatif aux élections et votations et d'autre part en leur proposant un questionnaire qui a rencontré un large écho dans les médias.

Fin 2018, les autorités de protection des données de la Confédération et des cantons ont publié un guide concernant l'application du droit de la protection des données au traitement numérique des données personnelles dans le cadre d'élections et de votations. L'objectif était d'inciter les partis politiques et autres acteurs tels que les opérateurs de réseaux sociaux et les commerçants de données à traiter les données conformément à la loi, dans la perspective des élections fédérales de 2019 ; ce guide montre aux partis politiques comment appliquer le principe de transparence conformément à la législation sur la protection des données afin de répondre aux attentes légitimes des électeurs (voir 26e Rapport, ch. 1.1).

Avant la phase finale de la campagne électorale, le Préposé a effectué une mise à jour de ce guide et l'a complété par une checklist destinée aux partis politiques. Cette liste, présentée sous forme de questionnaire, a rencontré un grand écho médiatique et amené plusieurs partis à améliorer leurs sites Internet avant le scrutin, dans le souci d'appliquer la loi sur la protection des données de manière exemplaire.

d'autres lacunes quant au respect de la législation sur la protection des données, il a renoncé à prendre de mesures supplémentaires.

Nous soulignons aujourd'hui à nouveau, après les élections de 2019, l'importance de préserver les droits de la personnalité dans le contexte politique. Nous continuerons à suivre la situation en Suisse à cet égard dans le cadre de notre mission de surveillance.

Identité électronique : Engagement pour un niveau de protection aussi élevé que possible

Avec la loi fédérale sur les services d'identification électronique (LSIE) une base légale a été créée afin de permettre une identification sûre des personnes dans les transactions commerciales en ligne ou dans les services en ligne des administrations publiques. Le Préposé a pu faire valoir ses préoccupations au cours du processus législatif.

Le partage des tâches entre l'État et les entreprises privées est demeuré un élément politiquement controversé au cours des travaux parlementaires sur la LSIE, aujourd'hui terminés : en tant que fournisseurs d'identité (IdP), des entreprises privées peuvent être autorisées à délivrer des identités électroniques dans le cadre juridique standardisé de la LSIE. La condition préalable à cette autorisation est une reconnaissance donnée par l'État à travers une commission indépendante, l'EIDCOM (Commission fédérale des e-ID). L'EIDCOM accorde cette certification aux acteurs privés qui offrent une garantie qu'ils répondent aux exigences techniques et sécuritaires de la LSIE. Avant de reconnaître un fournisseur d'identité, l'EIDCOM consulte le Préposé quant aux obligations de protection des données. Le fournisseur d'identité reconnu est soumis à la surveillance permanente de l'EIDCOM.

Dans le cadre de la préparation du projet par l'administration et des délibérations au sein des commissions juridiques des Chambres fédérales, le Préposé est intervenu afin que la LSIE n'impose pas d'obligation de s'identifier de manière sûre pour accéder à Internet ou au commerce en ligne. Notre autorité a également veillé à ce que le fournisseur d'identité ne communique pas de données à des tiers à des fins commerciales ou similaires. La communication de données à un fournisseur de services en ligne n'est autorisée que si elle est nécessaire à l'identification de la personne concernée auprès du fournisseur de services afin qu'il puisse remplir ses obligations contractuelles et si l'utilisateur en a été informé avant la première communication de données. Cette communication des données doit être régie par un accord entre le fournisseur d'identité et le fournisseur de services en ligne et doit également être soumise à l'examen du Préposé. Nos requêtes ayant été prises en compte au cours du processus législatif, le Préposé considère que la LSIE est conforme à la législation sur la protection des données de la Confédération.

Au cours des votations finales du 27 septembre 2019, le Conseil national et le Conseil des États ont adopté la LSIE. Le référendum contre cette loi a abouti. Il vise à placer la délivrance de l'identité électronique entre les seules mains de l'État.

SwissID

Avec « SwissID », la SwissSign Group SA est devenue une entreprise d'importance systémique. Le Préposé suit le projet dans le cadre de ses activités de conseil et de surveillance.

Avec SwissID, SwissSign Group SA propose pour les transactions commerciales en ligne un produit comprenant à la fois de purs services SSO (single sign on/authentification unique) et l'émission d'une identité électronique (voir l'article principal) sur une base privée. Dans la perspective de l'entrée en vigueur de la LSIE, SwissID doit être développé afin que les utilisateurs puissent procéder en ligne à des transactions juridiques exigeant une identification sur la base d'une identité électronique reconnue par l'État et obtenir des prestations de service public en ligne.

SwissSign Group ayant nommé un service garant de la protection des données dans l'entreprise et chargé ce service d'analyser les risques au regard du droit de la protection des données, le Préposé s'est concentré dans un premier temps, au cours de l'année sous revue et à l'occasion des rencontres régulières avec les responsables du projet, sur la possibilité de connexion anonyme pour les purs services SSO : les clients doivent pouvoir se connecter avec des informations fournies par elles-mêmes et n'être soumis ni à une obligation de vérité, ni à une procédure d'identification.

En outre, l'entreprise doit veiller à ce que les données personnelles d'identification ne soient transmises au fournisseur de services en ligne que si ce dernier en a absolument besoin pour l'exécution de sa transaction juridique. Ce principe ne doit pas pouvoir être renversé par un nouveau consentement de l'utilisateur.

SwissSign Group a garanti au Préposé qu'il allait intégrer ces principes dans sa politique en matière de données et qu'il les mettrait en œuvre dans les contrats avec les fournisseurs de services en ligne et les utilisateurs de SwissID.

La désanonymisation, un danger de l'intelligence artificielle

Un groupe de travail de la Confédération, auquel participe le Préposé, a formulé des exigences en matière de protection des données pour l'intelligence artificielle (IA). L'un des risques particuliers des systèmes d'IA est que des données personnelles peuvent être obtenues par la combinaison de données non personnelles.

Dans le cadre de la stratégie révisée « Suisse numérique », le Conseil fédéral a décidé de créer un groupe de travail interdépartemental dédié à l'intelligence artificielle (IA). Dans ce contexte, des groupes de projet ont été formés sur des thèmes spécifiques liés à l'intelligence artificielle. Le Préposé a participé au groupe de projet traitant de la disponibilité et de l'utilisation des données ainsi que des conditions-cadres et de la sécurité juridique.

Selon le rapport général du groupe de travail, les systèmes d'IA sont capables de déduire des informations personnelles à partir d'une combinaison d'éléments de données non personnelles qu'ils filtrent à partir d'énormes quantités de données (les mégadonnées, en anglais big data), ce qui conduit à la traçabilité de certaines personnes, rendant leur identification possible (désanonymisation). Ce rapport a été remis au Conseil fédéral en décembre 2019 et publié par le Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI (cfr. site du SEFRI).

Office fédéral de la statistique : amélioration de la transparence et audits requis pour la communication de données personnelles à l'étranger

L'Office fédéral de la statistique (OFS) a récemment choisi un prestataire de services de scannage qui remplit à l'étranger certaines parties de sa prestation contractuelle. À propos de la communication de données personnelles à l'étranger qui en résulte, le Préposé considère que les mesures de protection des données personnelles à l'étranger, qui reposent sur des accords contractuels, sont appropriées au regard des règles de protection des données. Toutefois, il demande plus de transparence pour les personnes concernées et requiert que des contrôles (audits) soient effectués sur place auprès des sous-traitants.

En raison de la fermeture du service de numérisation et de scannage de l'Office fédéral de l'informatique et des télécommunications à la fin de 2018, l'Office fédéral de la statistique, en collaboration avec l'Office fédéral des constructions et de la logistique, a été chargé d'évaluer un nouveau fournisseur de services de scannage dans le cadre d'une procédure d'adjudication OMC. Après la mise en œuvre de cette procédure, le mandat a été attribué à la société « Tessi document solutions GmbH ». Le scannage des documents papier est effectué sur le site de Genève, où ces documents sont ensuite soit détruits de manière sécurisée, soit renvoyés à l'OFS. Les questionnaires papier ne quittent donc pas la Suisse.

Après le processus de numérisation, les champs de texte reconnus comme incorrects (extraits des documents) sont corrigés manuellement à l'étranger. La solution de traitement électronique retenue à cet effet ne présente à l'utilisateur à l'étranger que l'image des champs de texte à corriger, le document complet restant en Suisse dans les systèmes. Il y a donc communication transfrontière de données au sens de l'art. 6, LPD. L'OFS a transmis au Préposé une documentation complète à ce sujet, ainsi que les accords contractuels qui montrent que d'importantes mesures techniques, organisationnelles et contractuelles ont été prises pour protéger les données personnelles à l'étranger. Le Préposé a répondu en précisant que l'OFS, en tant que mandant, est responsable de la protection et de la sécurité des données tout au long de la chaîne de traitement et que, conformément à l'art. 10a, al. 2, LPD, il doit également s'assurer que le tiers mandataire garantit la sécurité des données. En outre, compte tenu de la portée de ce projet, le Préposé a jugé opportun d'effectuer des contrôles aléatoires dans les locaux où les données sont traitées.

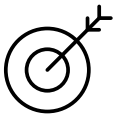
Par ailleurs, le Préposé considère qu'il est indispensable, conformément au principe de transparence inscrit dans le droit de la protection des données, que les personnes concernées soient activement informées par l'OFS du fait que leurs données sont communiquées à l'étranger. Selon lui, l'information des personnes concernées doit se faire par une référence idoine dans les questionnaires d'enquête de l'OFS.

Il s'avère que les considérations relatives à la protection des données doivent déjà être incluses dans la phase d'évaluation OMC des projets impliquant des traitements de données personnelles. Le Préposé poursuivra l'accompagnement du projet et vérifiera l'application des mesures requises.

Pour le Préposé, la commercialisation des données de déplacement provenant de téléphones mobiles demeure problématique malgré une anonymisation complexe

La manière dont chaque individu se déplace est unique en soi. C'est pourquoi, même après la mise en œuvre de méthodes d'anonymisation sophistiquées, on ne peut exclure, au moins dans certains cas, que des personnes puissent être aisément identifiées sur la base de ce schéma clair de déplacement, associé à des informations supplémentaires. Les données concernées doivent donc être qualifiées de données personnelles, dont le traitement requiert le consentement des personnes concernées et doivent être protégées en conséquence.

Dans le secteur commercial, une tendance se poursuit, consistant à utiliser à des fins statistiques les données de déplacement provenant de téléphones mobiles. Ainsi, aujourd'hui, grâce à ces données, les responsables des traitements peuvent localiser avec précision en quel endroit les citoyens se promènent, conduisent, prennent l'avion ou utilisent les transports publics.



Ces données de déplacement sont utilisées par exemple pour améliorer les flux de circulation ou planifier l'emplacement optimal d'un magasin.

En 2019, le Préposé a reçu de la part d'une entreprise une demande concernant l'utilisation de données de déplacement. La question était de savoir si les données encore classées comme données personnelles malgré l'application d'une méthode d'anonymisation décrite en détail dans la documentation peuvent être transférées du fournisseur de téléphonie mobile à l'entreprise en question. Cette méthode prévoit déjà plusieurs étapes d'anonymisation dans les locaux du fournisseur de services de télécommunications afin que l'entreprise ne reçoive que des données statistiques sur le comportement des individus. D'une part, les informations sur la localisation des appareils de téléphonie mobile ne sont pas enregistrées avec une précision extrême. D'autre part, les trajets possibles sont calculés à partir de ces données de localisation imprécises et celui présentant la plus grande probabilité est sélectionné. Il en résulte des profils de mouvement qui correspondent aux habitudes régulières de la population, mais qui ne sont pas destinés à refléter le comportement effectif d'un individu.

Selon l'évaluation du Préposé, la méthode d'anonymisation de l'entreprise réduit considérablement les possibilités de réidentification des personnes.

Toutefois, on ne peut exclure la possibilité de tirer des conclusions sur un individu concret à partir des données transmises et de l'agrégation domicile/lieu de travail. Le problème se pose en particulier dans les régions rurales à faible densité de population. Or, selon le Préposé, une réidentification ne nécessite pas des moyens vraiment très importants, donc on peut s'attendre, selon l'expérience générale de la vie, à ce qu'une personne intéressée les mette en œuvre. Pour cette raison, on ne peut exclure qu'il soit possible d'identifier aisément un individu sur la base des données disponibles associées à d'autres informations, et que par conséquent nous soyons en présence de données personnelles au sens de l'art. 3, let. a, LPD.

En l'occurrence, les données personnelles collectées dans le but de fournir des services de télécommunication et de les facturer sont utilisées à d'autres fins. Cette modification de la finalité du traitement implique que le consentement des personnes concernées doit être obtenu et que des mesures doivent être prises pour protéger les données personnelles.

Norme 5G : le Préposé contrôle les mesures de protection des données des fournisseur de services de télécommunication visant à garantir un déploiement sécurisé

Le Préposé a entrepris des vérifications techniques concernant l'implémentation de la nouvelle norme de télécommunication 5G en conformité avec la protection des données.

La nouvelle norme de télécommunication 5G, qui succède à l'actuelle norme 4G/LTE, promet non seulement une plus grande largeur de bande et la possibilité de connecter un plus grand nombre d'appareils simultanément, mais aussi des transmissions de données pratiquement en temps réel. Ainsi, la norme de télécommunications 5G constitue la base d'une multitude d'applications futures, par exemple dans l'industrie avec les capteurs IoT (Internet des objets) ou les véhicules connectés. Bien que la 5G soit une norme internationale pour l'Internet et la téléphonie mobile, il existe de grandes différences dans sa mise en œuvre par les différents fournisseurs. En outre, des rapports publics de chercheurs de l'EPFZ [arXiv : 1806.10360v3 [cs.CR] 18 oct. 2018] d'une part et des universités de Purdue (Indiana) et de l'Iowa [NDSS '19, 24-27 février 2019, San Diego, CA, USA Copyright 2019 Internet Society, ISBN 1-891562-55-X] d'autre part, mettent en lumière les failles de sécurité de la nouvelle norme 5G (entre autres dans les messages de pagination avec les attaques ToRPEDO et PIERCER). Selon ces rapports toutefois, la nouvelle norme est censée être globalement plus sûre que la norme 4G précédente.

La documentation remise au Préposé sur le déploiement de la 5G et ses vérifications sur place lui ont permis de se faire une idée précise du niveau de sécurité et des mesures prises. Ces inspections n'étaient pas encore été terminées au cours de l'année sous revue.

Erreurs d'adresses électroniques chez Swisscom

Une panne dans l'un des systèmes clients de Swisscom a entraîné l'envoi de courriers électroniques à des adresses erronées. La société a rapidement pris les mesures nécessaires.

Un particulier, client de Swisscom, a informé le Préposé qu'il avait reçu divers courriers électroniques qui ne lui étaient pas destinés. Le Préposé a demandé des explications à Swisscom. L'entreprise a déclaré qu'elle était déjà au courant du problème et avait chargé un groupe de travail d'effectuer une analyse des risques. Il est apparu que les adresses électroniques enregistrées de manière générique dans l'un des systèmes clients de Swisscom n'étaient pas attribuées aux bons clients. En conséquence, certains e-mails de Swisscom avaient été envoyés à des adresses erronées. Une fois l'incident connu, l'entreprise a supprimé ces courriers électroniques des comptes des destinataires concernés.

Entre-temps, Swisscom a aussi identifié les adresses électroniques mal attribuées et immédiatement veillé à ce qu'elle n'envoie plus de courriels à ces adresses. Swisscom a de plus précisé que rien n'indiquait que les courriels mal adressés aient été utilisés de manière abusive. L'entreprise est également en train d'adapter ses processus afin d'éviter que de tels incidents ne se reproduisent.

Le Préposé a pris note des mesures immédiates prises par Swisscom sur la base de l'analyse des risques et, s'appuyant sur ces mesures, n'a pas recommandé d'autres actions

Tiktok dans le collimateur des autorités de protection des données

La plateforme de partage de vidéos Tiktok est extrêmement populaire auprès des enfants et des jeunes. Les conditions d'utilisation n'étant pas claires pour les clients suisses, le Préposé a contacté l'opérateur chinois de l'application. En outre, il est en contact avec l'autorité britannique de protection des données afin de clarifier les questions concernant la protection de la personnalité des utilisateurs.

Tiktok est une plateforme de partage de vidéos particulièrement populaire auprès des jeunes, avec des taux de téléchargement en augmentation extrêmement rapide dans les Appstores respectifs. Elle permet aux jeunes utilisateurs de créer eux-mêmes de courts clips agrémentés de divers effets et filtres et de les partager. Les fonctions de la plateforme en tant que réseau social permettent de contacter très facilement d'autres utilisateurs, de réagir à leurs vidéos et de les commenter.

Cette application est la propriété de la société chinoise de technologie Internet Bytedance, basée à Pékin. Les médias se sont fait l'écho de diverses réserves et critiques à l'encontre du propriétaire du portail vidéo. Par exemple, ils l'accusent de ne pas protéger suffisamment la sphère privée des enfants ou de censurer ou filtrer certains contenus selon les instructions des autorités chinoises.

Le Préposé a constaté que les utilisateurs suisses ne savent pas clairement quelles conditions d'utilisation leur sont applicables car celles-ci se réfèrent à la zone UE. Il a demandé au service responsable de Tiktok de se prononcer à ce propos et de lui préciser quelles étaient les mesures visant à protéger les enfants et les jeunes. En outre, il a demandé que la société désigne un service qui puisse fournir des informations sur les questions de protection des données.

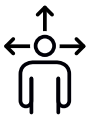
La société a répondu aux questions du Préposé et nommé un interlocuteur. Par ailleurs, le Préposé est en relation avec l'autorité britannique de protection des données qui, au cours de l'année sous revue, a ouvert une procédure contre Tiktok au sujet de la protection des enfants et des jeunes et du traitement de leurs données.

Service de streaming musical – Analyse de données personnelles à la suite d'une demande de renseignements du Préposé

Un service de streaming musical a demandé à avoir accès aux données GPS de ses utilisateurs pour vérifier leur adresse personnelle. Dans le cadre de ses investigations, le Préposé a demandé des informations et a analysé en détail les données reçues. La clarification du cas a été close sans autres mesures formelles.

Au cours de l'année sous revue, un service de streaming musical très connu a fait l'objet dans la presse de divers articles rapportant que ses utilisateurs avaient été récemment invités à transmettre leur localisation grâce aux coordonnées GPS de leurs smartphones, cela dans le but de vérifier leur appartenance à un ménage à des fins de facturation. Ce fait a incité le Préposé à vérifier la licéité de ce traitement de données ; il a donc demandé à ce service de streaming musical de lui fournir des données d'utilisation concrètes. Notre analyse de ces données a montré que le fournisseur traitait les données d'utilisation qui lui étaient transmises conformément à ses propres règles d'utilisation et de protection des données. Nous avons aussi examiné ces règles qui, de notre point de vue, sont formulées de manière compréhensible et conformes aux exigences légales. Aucune anomalie n'a été relevée à cet égard.

Le consentement relatif à la transmission des données GPS de l'utilisateur au fournisseur figure dans la déclaration de politique de protection des données comme étant un consentement volontaire. En effet, au moment de la demande, l'utilisateur a le choix d'envoyer la confirmation demandée



soit par signal GPS, soit par transmission de son code postal. De ce fait, le client n'étant pas tenu de transmettre ses données GPS au service de streaming musical, le Préposé estime qu'il n'y a pas lieu de contester le processus.

La durée de conservation des données d'utilisateur a été aussi examinée. Une distinction est faite ici entre les données d'utilisateur et les données d'utilisation :

- Les données d'utilisateur sont saisies lors de la création du compte utilisateur (compte du client) et contiennent des informations d'identité et de contact qui sont utilisées et conservées pendant toute la durée du service. Ces informations sont nécessaires pour les contacts et l'établissement correct des factures. En ce qui concerne les données GPS demandées par la société de streaming pour la détermination de l'emplacement, aucune donnée de ce type n'a été trouvée dans les données d'utilisateur reçues. La suppression de ses propres données d'utilisateur ne peut être obtenue que par la fermeture définitive du compte, donc par la renonciation à l'utilisation du service de streaming. Il n'y donc pas lieu de contester ce processus car en raison des prescriptions sur les droits d'auteur, il est impossible d'utiliser l'offre de streaming sans être enregistré.
- La situation est différente quant aux données d'utilisation. Celles-ci sont créées durant l'utilisation du service et contiennent des informations sur cette utilisation. Bien que ces informations améliorent l'expérience utilisateur, elles ne sont pas absolument nécessaires à la gestion des utilisateurs. Pour cette raison, le contrôle des données d'utilisation est possible car l'utilisateur peut en tout temps supprimer lui-même les données qu'il a aussi lui-même produites, par exemple ses listes de lecture. Les autres données d'utilisation, comme l'historique des écoutes, sont stockées pendant une période de 90 jours et sont ensuite automatiquement supprimées. Cette manière de procéder est proportionnée et n'est pas contraire aux exigences légales.

Le Préposé n'ayant constaté aucune action disproportionnée de la part de ce service de streaming musical, la clarification des faits a été close sans autres mesures formelles.

Clearview se procure des images faciales sans le consentement des intéressés

Sur son site Internet, le Préposé a publié plusieurs mises en garde contre la menace d'atteintes à la personnalité en Suisse, due à la collecte d'images faciales sur Internet, sans le consentement des personnes concernées.
Selon plusieurs articles de presse, les fournisseurs américains de l'application Clearview gèrent une banque de données de quelque trois milliards d'images faciales, qu'ils obtiennent en exploitant Internet et les réseaux sociaux. Le modèle commercial de Clearview consiste à comparer, pour ses clients abonnés, une image faciale avec sa banque de données et, sur la base d'informations supplémentaires, à attribuer les correspondances positives à des personnes identifiables. Les clients américains de Clearview seraient notamment des autorités de police.

Comme nous nous attendions à ce que la base de données de Clearview traite également les images faciales de résidents suisses, le Préposé a pris position sur son site en janvier 2020 à propos de l'application Clearview : il a précisé à l'intention de Clearview que la loi fédérale sur la protection des données et la personnalité des personnes concernées seraient gravement violées en Suisse si leurs images faciales étaient collectées sans leur consentement et ensuite traitées pour le compte d'autorités de police étrangères. Il a indiqué aux réseaux sociaux, dont les conditions d'utilisation interdisent généralement la récupération non sollicitée de données sur leurs plateformes par des tiers ou des robots, qu'ils doivent assurer une meilleure protection technique des données d'image de leurs clients. Enfin, le Préposé a recommandé aux utilisateurs des réseaux sociaux de faire preuve de responsabilité et de paramétrer leur compte de sorte à empêcher que des moteurs de recherche puissent accéder à leurs photos.

Afin de pouvoir évaluer dans quelle mesure la population suisse était touchée, le Préposé a déposé, le 24 janvier 2020, une demande d'accès et d'effacement des données traitées sur sa personne auprès de Clearview. Malgré plusieurs rappels, cette demande était encore sans réponse à la fin de la période sous revue. Dans un délai raisonnable, les directions de l'Office fédéral de la police (fedpol), de l'Administration fédérale des douanes (AFD) et du Service de renseignement de la Confédération (SRC) ont toutefois confirmé au Préposé, à la demande de ce dernier, qu'elles n'utilisaient pas ou n'ont pas l'intention d'utiliser Clearview ou des applications comparables dans le cadre de leurs activités.

Le Préposé fera usage de tous les moyens que lui confère la loi pour protéger la population suisse contre la collecte non consentie de données faciales afin que tout un chacun puisse continuer à se déplacer en tout anonymat, aussi bien dans l'espace virtuel que réel.

Révision de la loi fédérale sur la protection des données

Au cours de l'année écoulée, la révision totale de la Loi fédérale sur la protection des données du 19 juin 1992 (LPD) a franchi d'importantes étapes. Après avoir été examiné successivement par la Commission des institutions politiques du Conseil National et son homologue du Conseil des Etats, le projet se trouve désormais dans la phase d'élimination des divergences. La situation extraordinaire liée à la pandémie du Covid-19 que nous traversons perturbe le déroulement du processus législatif et retardera vraisemblablement l'adoption de la révision. La loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS), entrée en vigueur le 1er mars 2019 à titre provisoire, devra donc attendre avant d'être formellement abrogée et matériellement intégrée à la nouvelle LPD.

Lors des interventions auprès des Commissions parlementaires auxquelles il a été convié, le Préposé a préconisé l'adoption de mesures aptes à faire face au développement dynamique des technologies et des risques qui y sont associés. Il a défendu les propositions offrant aux Suissesses et Suisses un niveau de protection équivalent à la Convention du Conseil de l'Europe sur la protection des données (Convention 108+) et similaire au Règlement européen sur la protection des données (RGPD) déjà appliqué par de nombreux acteurs en Suisse en faveur de leur clientèle à titre de « best practice ».

Dans le prolongement de l'approche actuelle de protection des données, le projet prévoit ainsi un renforcement de ses principes fondamentaux comme la protection des données par défaut (privacy by default) et dès la conception (privacy by design) qui s'ajoutent aux principes préexistants. En outre, la terminologie a été modernisée et alignée sur celle du droit européen, laissant toutefois subsister des divergences susceptibles d'engendrer une certaine insécurité juridique et des difficultés d'application pratique. Certaines d'entre elles révèlent de véritables différences conceptuelles, telle les définitions de « profilage » et « profilage à risque élevé », une innovation du Conseil des Etats et divergence majeure d'avec le Conseil national.

Cette refonte permet ainsi à la Suisse d'honorer les engagements pris lors de la récente signature de la Convention 108+ et – comme on peut l'espérer - de faire bénéficier son économie d'une décision d'adéquation qui lui conserve un plein accès au marché européen.

Convention 108+ du Conseil de l'Europe pour la protection des données personnelles

En octobre 2019, le Conseil fédéral a décidé de signer le Protocole d'amendement à la Convention 108 du Conseil de l'Europe pour la protection des données à caractère personnel (Convention 108+). La Suisse a ensuite officiellement signé la Convention 108+ le 21 novembre 2019 à Strasbourg. Le message à l'intention du Parlement portant approbation dudit protocole a été adopté par le Conseil fédéral le 6 décembre 2019. Par sa signature, la Suisse entend garantir un niveau de protection des données reconnu au plan international.

Le Préposé a souligné dans le 26e Rapport d'activités 2018/19 qu'il serait opportun que le Conseil fédéral signe la nouvelle version de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Le 2 octobre 1997, la Suisse a ratifié dans sa forme initiale la Convention du Conseil de l'Europe sur la protection des données, entrée en vigueur en 1985. Cette Convention a été remaniée par le Conseil de l'Europe au cours des dernières années afin de répondre à l'évolution des technologies et aux défis de la numérisation. Le protocole d'amendement est ouvert à la signature depuis octobre 2018. À ce jour, plus d'une trentaine d'États l'ont signé et certains l'ont déjà ratifié.

L'adhésion à la Convention modernisée du Conseil de l'Europe sur la protection des données revêt une grande importance pour la Suisse. Elle renforce dans notre pays la protection des citoyens dont les données personnelles sont traitées dans l'un des États parties. En outre, elle simplifie l'échange de données entre États parties et garantit que la transmission transfrontière de données reste possible sans que des garanties supplémentaires soient nécessaires. Par ailleurs, la Convention 108+ revêt une grande importance dans la mesure où elle influencera la décision d'adéquation que prendra prochainement l'UE à propos du niveau de protection des données en Suisse. En effet, comme elle le fait pour tous les États tiers, l'UE tiendra compte du fait que l'État examiné est partie à la Convention.

La Convention 108+ étend les obligations du responsable du traitement des données. Celui-ci est notamment tenu d'annoncer à l'autorité de contrôle compétente certains cas de violation de la protection des données. Les droits des personnes concernées sont également renforcés, puisque le responsable du traitement doit, dans certains cas, informer la personne concernée de la collecte de ses données personnelles. En outre, toujours en vertu de cette nouvelle Convention 108+, le responsable du traitement des données devra procéder à une analyse d'impact relative à la protection des données personnelles avant certains traitements. La protection des données doit être intégrée à un projet dès sa conception (privacy by design) et les paramètres par défaut doivent être configurés de manière à respecter la protection des données. Le protocole d'amendement prévoit également un renforcement des droits des personnes concernées, notamment en ce qui concerne leur droit d'accès et leur droit d'opposition en cas de décision individuelle automatisée. Il impose aussi aux États parties d'établir un système de sanctions et un système de recours et de conférer aux autorités de contrôle la compétence de rendre des décisions contraignantes.

Le 30 octobre 2019, le Conseil fédéral a décidé de signer la Convention 108+. La Suisse a ensuite officiellement signé la Convention à Strasbourg le 21 novembre suivant. Par la suite, lors de sa séance du 6 décembre 2019, le Conseil fédéral a adopté à l'intention du Parlement le message relatif à l'approbation du protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le Parlement doit se prononcer sur sa ratification.

L'adhésion à la Convention modernisée permet à la Suisse de garantir un niveau élevé de protection des données dans la sphère privée et de faciliter le flux transfrontière de données dans les secteurs public et privé, ce qui est également dans l'intérêt de l'économie suisse.


Arrival 2
Taxi
Lost & Found 1|2
Check-in 2

1.2 Justice, police, sécurité

Profils d'ADN : un cadre légal strict est indispensable

Dans le cadre de la consultation des offices relative au projet de modification de la loi sur les profils d'ADN, le Préposé a salué de manière générale les changements et nouveautés proposés. Il a demandé cependant de prévoir un cadre légal strict pour les nouveaux instruments que sont la recherche élargie en parentèle et le phénotypage.
Le projet de modification du Département fédéral de justice et police (DFJP) prévoit une séparation des dispositions relevant d'une part de la loi sur les profils d'ADN et, d'autre part de celles relevant des codes de procédures pénales civile et militaire. Le Préposé a salué cette proposition de clarification.

Une nouvelle solution en matière de conservation des profils d'ADN est également proposée. Celle-ci tient compte du principe de proportionnalité et des exigences spécifiques contenues dans le droit pénal des mineurs.

En ce qui concerne la recherche élargie en parentèle et le phénotypage, le Préposé exige que des conditions strictes permettent de garantir la proportionnalité des atteintes aux droits fondamentaux des personnes concernées. Le Préposé est d'avis que ces instruments doivent être considérés comme des solutions de dernier recours. Ceux-ci ne doivent être utilisés que pour élucider des cas de crimes graves en fonction de la nature des biens juridiques concernés, comme les crimes contre la vie et l'intégrité corporelle, contre la liberté, ou contre l'intégrité sexuelle. Par contre, la recherche élargie en parentèle et le phénotypage de même que les enquêtes de grande envergure ne devraient, en règle générale, pas être mis en œuvre dans les cas de crimes contre le patrimoine. En matière de phénotypage, la détermination de certains éléments, comme par exemple la couleur des cheveux, n'est pas assez précise et pourrait être problématique par rapport au principe d'exactitude des données. Dans le cadre de la recherche élargie en parentèle, la collecte de données constitue une violation du droit de refuser de témoigner qui ne peut être justifiée que pour les crimes les plus graves.

Comme indiqué ci-dessus, la recherche élargie en parentèle et le phénotypage doivent être utilisés pour les crimes les plus graves en fonction de la nature des biens juridiques concernés. Etant difficiles d'établir une liste exhaustive de crimes permettant de telles mesures, le Préposé a proposé que celles-ci soient décidées par le tribunal des mesures de contrainte comme cela est déjà le cas pour les enquêtes de grande envergure. Le Conseil fédéral n'a pas retenu la proposition du Préposé et ce dernier, s'il est sollicité, se prononcera dans le cadre des travaux parlementaires.

Report de la loi sur la communication de données de passagers aériens dans les États membres de l'UE

Le Préposé a continué à accompagner les travaux de création d'une base légale portant sur la communication des données PNR par les compagnies aériennes aux États membres de l'UE. Nous avons souligné à plusieurs reprises l'urgence de disposer d'un cadre légal dans les meilleurs délais.
Comme le Préposé l'a relevé dans le Rapport d'activités 2018/19, plusieurs pays de l'UE prévoient d'exiger des compagnies aériennes qu'elles fournissent des données sur les passagers des vols en provenance de Suisse. Ils se basent sur la Directive européenne 2016/681 du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (Directive PNR de l'UE).

Nous avions fait remarquer aux autorités fédérales compétentes qu'il fallait pour cela créer une base légale. Il a été promis au Préposé que la base légale pour la fourniture de données PNR aux États qui en auraient besoin conformément à la Directive PNR de l'UE serait créée par une révision de l'ordonnance sur l'aviation (cf. 26e Rapport, ch. 1.2)

L'Office fédéral de l'aviation civile (OFAC), en tant qu'office fédéral compétent, a alors entamé les travaux législatifs correspondants. Dès le début, le Préposé est resté à la disposition de l'OFAC à titre consultatif jusqu'à ce que l'Office décide de reporter ses travaux. L'OFAC a fait valoir d'une part que les travaux réalisés jusqu'à présent avaient montré qu'une base légale devait d'abord être créée dans une loi formelle. Et d'autre part qu'il fallait s'attendre à ce que le Conseil fédéral arrête prochainement, dans un projet de loi séparé, la procédure ultérieure quant à l'utilisation par la Suisse des données de passagers aériens pour lutter contre la grande criminalité et le terrorisme. Et qu'enfin, il était donc logique de combiner les deux projets et de les traiter simultanément.

Le Préposé a de nouveau souligné l'urgence de créer une base légale. Sans elle, la communication de données PNR par les compagnies aériennes aux autorités de l'UE serait illicite. Par souci d'exhaustivité, nous avons également relevé que la communication de données PNR par les compagnies aériennes à des pays tiers (c'est-à-dire en dehors du champ d'application de la Directive PNR de l'UE) devrait reposer sur la création d'accords. À la suite de cela, l'Office fédéral de la police a entamé ses travaux sur la réglementation légale de l'utilisation des données des passagers aériens par les autorités suisses dans la lutte contre la grande criminalité et le terrorisme.

La question de la communication de données de passagers aériens aux États de l'UE sur la base de la Directive PNR de l'UE y a aussi été intégrée. Le Préposé s'est également prononcé dans le cadre de la consultation des offices et a maintenu sa position antérieure. En février 2020, le Conseil fédéral s'est prononcé dans une décision de principe en faveur de l'utilisation des données des passagers aériens en Suisse pour lutter contre le terrorisme et la criminalité. Le Préposé continuera d'accompagner les travaux législatifs à titre consultatif.

Système de réservation de Swiss – Mise en œuvre de mesures contre l'utilisation abusive de données

Le PFPDT a déjà abordé la question du système de réservation de la compagnie aérienne Swiss. L'entreprise a promis de mettre en œuvre certains ajustements – comme le masquage partiel du numéro de passeport – en parallèle au lancement de son nouveau site web, qui a toutefois été retardé.

Comme le mentionnait notre précédent rapport d'activités, la compagnie aérienne Swiss a modifié ses Conditions Générales de Transport (CGT) à la demande du Préposé afin de sensibiliser ses clients à la nécessité de protéger les données personnelles visibles ou stockées sur la carte d'embarquement. En outre, le numéro de passeport, qui dans certains cas est visible lors de la consultation de la réservation, devrait être rendu partiellement illisible (cf. 26e Rapport, ch. 1.2). Swiss a informé le Préposé que ces ajustements seraient mis en œuvre parallèlement au lancement de son nouveau site web. Toutefois, le passage à la nouvelle architecture du site et le masquage du numéro de passeport qui y est associé ont été retardés. Swiss a donc décidé d'introduire séparément et à l'avance, le masquage des numéros de passeport ainsi que, et cela est nouveau, des données de visa et de GreenCard sur son site web en permettant de lire les deux premiers caractères des numéros de passeport ainsi que des données de visa et de GreenCard lors de la réservation, et en remplaçant tous les caractères suivants par un « x ». Swiss a mis en œuvre ces changements à la fin de l'année 2019.

Mesures policières contre le terrorisme

Avant de proposer de nouvelles réglementations, il aurait été absolument nécessaire d'élaborer une loi sur la police au niveau de la Confédération. En conséquence, le Préposé remet en question dans son ensemble le projet de réglementation en matière de mesures policières contre le terrorisme.

Dans ses rapports d'activités, le Préposé déplore depuis plusieurs années de la fragmentation des bases légales régissant les activités des autorités fédérales en matière de police. En effet, contrairement aux cantons, la Confédération ne dispose pas d'une loi sur la police au sens d'une codification complète des tâches, des compétences et du traitement des données personnelles. L'Office fédéral de la police (fedpol) gère un grand nombre de bases d'informations qui permettent le traitement centralisé de données extrêmement sensibles que les autorités policières fédérales et cantonales échangent entre elles et avec d'autres pays.

Le traitement des données repose sur un ensemble confus de lois spéciales que même des juristes spécialisés, sans parler du personnel de police au front, ont de la peine à appliquer et même l'instruction en matière de traitement des données a depuis longtemps atteint ses limites compte tenu de la complexité.

Au lieu d'élaborer une loi sur les tâches de police ou du moins d'une loi sur l'information et la coopération au niveau fédéral, le DFJP crée constamment de nouvelles réglementations comme celle sur les mesures policières contre le terrorisme ou celle sur les précurseurs d'explosifs, qui alourdissent la complexité déjà déraisonnable des réglementations et laissent parfois aussi ouvertes les questions suivantes: dans quels systèmes les données préventives doivent-elles être traitées, de quelle manière et pendant combien de temps ?

Compte tenu de cette situation, le Préposé n'est plus disposé à soutenir des projets législatifs sensibles comme les mesures policières contre le terrorisme dans la phase parlementaire. Le Préposé remet en question dans son ensemble le projet du DFJP. Cependant, malgré nos critiques publiées dans le dernier rapport annuel (cf. 26e Rapport, ch. 1.2) et dans les médias, la Commission du Conseil des États s'est abstenue d'entendre le Préposé sur cette question.

Contrôle technique de l'utilisation du Système d'Information Schengen chez la Fedpol et l'ISC-EJPD

En tant qu'autorité de surveillance du « Schengen Information System » (SIS) le PFPDT a effectué un contrôle technique auprès de la Fedpol et de l'ISC-EJPD.

Le N-SIS est la copie nationale suisse du SIS central (C-SIS). Le traitement des données dans le N-SIS ainsi que la transmission des données au SIS central sont décrites dans le règlement de traitement « Informationssystem N-SIS und dessen Teilsysteme ». En Suisse, plus de 30 000 utilisateurs de divers organes fédéraux (ex. RIPOL, SEM), cantonaux (ex. administrations et polices cantonales), et municipaux utilisent le N-SIS.

L'ISC-EJPD développe le système et fournit le service à la Fedpol, qui le gère. Nous avons effectué ce contrôle technique auprès des deux. D'autres organes tels que la RIPOL, SYMIC et des polices cantonales ont été contactés dans ce contexte sans être soumis à ce contrôle.

Le premier objectif de ce contrôle consiste à vérifier la conformité à l'état de l'art des mesures techniques et organisationnelle, inspirées principalement de l'ISO 27001, pour la sécurité et la protection des données dans le système et son utilisation. Le deuxième objectif du contrôle est de vérifier la mise en œuvre de ces mesures.

Les discussions autour de notre liste de questions et des éléments contrôlés nous ont amenés à approfondir des points spécifiques. À la fin de la période sous revue, le contrôle n'était pas encore achevé.


Check-in 3
Zuschauerterrasse
Observation Deck

Contrôle ouvert auprès de fedpol relatif aux activités du bureau SIRENE

En début d'année 2018, s'est déroulée l'évaluation de l'application, par la Suisse, de l'acquis de Schengen dans le domaine de la protection des données. Dans ce contexte, de même qu'en tant qu'autorité nationale de surveillance du fichier du N-SIS, le Préposé a procédé à un contrôle relatif aux activités du bureau SIRENE de fedpol.

Le Conseil de l'UE, sur proposition de la Commission, a décidé le 7 mars 2019 d'arrêter un certain nombre de recommandations pour remédier aux manquements constatés lors de l'évaluation de la Suisse. Certaines recommandations concernent le Préposé, dont notamment celle portant sur son activité de surveillance dans le SIS. Selon cette recommandation, le Préposé doit veiller à contrôler plus fréquemment la licéité des traitements des données personnelles du SIS et à effectuer, au moins tous les quatre ans, des audits des opérations de traitement des données dans la partie nationale du SIS (N-SIS).

Ces inspections ne devraient pas se limiter à la vérification des fichiers journaux, mais devraient également couvrir d'autres aspects de la structure et du fonctionnement du N-SIS relatifs à la protection des données et porter sur les opérations de traitement des données auprès du responsable du N-SIS, c'est-à-dire fedpol y compris le bureau SIRENE et le serveur N-SIS.

Dans ce contexte, de même que dans le cadre de ses activités de contrôle en relation avec la mise en œuvre de Schengen et en tant qu'autorité nationale de surveillance du fichier du N-SIS, le Préposé a ouvert, en juin 2019, un contrôle relatif aux activités du bureau SIRENE de fedpol en lien avec les signalements dans le SIS, ainsi que l'échange d'informations supplémentaires du bureau SIRENE avec ses homologues étrangers.

Après l'envoi d'un questionnaire sur les activités générales du bureau SIRENE, le Préposé a effectué une visite sur place afin de se faire présenter la gestion d'un signalement dans le système du bureau SIRENE ainsi que l'échange d'informations supplémentaires.

À l'issue de son contrôle, le Préposé est parvenu à la conclusion que le bureau SIRENE traite les données relatives aux signalements et l'échange d'informations supplémentaires dans le respect de l'application des dispositions de droit suisse adoptées en matière de protection des données dans les secteurs couverts par la Convention d'application Schengen du 19 juin 1990 de l'Accord de Schengen (CAAS) et du droit européen. Le Préposé n'a donc pas rendu de décision ou pris des mesures particulières dans ce cadre.

Son examen a ainsi porté sur

- la structure et la fonction du N-SIS ;
- la composition du bureau SIRENE et son système informatique SIRENE-IT ;
- l'octroi et la gestion des droits d'accès au N-SIS ;
- le contrôle des accès des collaborateurs du bureau SIRENE au N-SIS ;
- les tâches du bureau SIRENE dans le cadre de signalements dans le N-SIS, de même que dans le cadre de l'échange d'informations supplémentaires avec ses homologues étrangers, ainsi que la description de ses tâches dans le cadre d'une usurpation d'identité ;
- la conservation des signalements et des informations supplémentaires ;
- les droits d'accès, de rectification et d'effacement ;
- la formation et la sensibilisation des collaborateurs.

Il a ainsi pu mettre en œuvre la recommandation de l'évaluation Schengen 2018 et de ce fait remplir les conditions des art. 44 du Règlement SIS II[1] et 60 de la Décision SIS II[2].

Un second contrôle du Préposé portant plus précisément sur les aspects techniques et de sécurité des serveurs a été lancé auprès du Centre de services informatiques du DFJP (CSI-DFJP).

[1] Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) [Règlement SIS II].

[2] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) [Décision SIS II].

La loi fédérale sur la protection des données Schengen

La loi fédérale sur la protection des données Schengen (LPDS) est entrée en vigueur le 1er mars 2019 et avec elle des nouveautés touchant notamment aux compétences actuelles du Préposé (cf. 26e Rapport, ch. 1.2).

La LPDS s'applique en particulier aux traitements de données personnelles par les organes fédéraux à des fins de prévention et poursuite d'infractions pénales dans le cadre de la mise en œuvre de l'acquis de Schengen. Au vu des nouvelles exigences et de l'effet transversal que cette nouvelle loi a sur les activités des offices concernés, le Préposé a pris contact avec les conseillers à la protection des données des organes fédéraux susceptibles d'être assujettis à la LPDS et concernés en première ligne, notamment l'Office fédéral de la police (fedpol), l'Office fédéral de la justice dans le domaine de l'entraide judiciaire en matière pénale et le Ministère public de la Confédération, mais aussi le Secrétariat d'Etat à la migration et l'Administration fédérale des douanes. L'accent a été mis sur la clarification du champ d'application ainsi que les nouveautés introduites par cette législation. L'échange de vues a notamment porté sur les traitements de données et les organes fédéraux assujettis à la LPDS, de même que sur les compétences du Préposé. Ce dernier reste en contact permanent avec les organes fédéraux concernés dans le cadre de la mise en œuvre de la LPDS dans leur champ d'activité respectif.

L'article 21 LPDS confère au Préposé la charge de surveiller l'application des dispositions fédérales relatives à la protection des données. Avant de planifier des contrôles selon les articles 21 à 25 LPDS, le Préposé souhaite avoir une vue d'ensemble des activités de traitement soumis à la LPDS (fichiers/systèmes d'information).

Pour cette raison, il a demandé à l'Office fédéral de la police (fedpol) et à l'Administration fédérale des douanes de nous fournir une copie du registre des activités de traitement au sens de l'article 12 LPDS et si elles existent ou si elles peuvent être générées, des indications statistiques par activité de traitement (fichier/système d'information) pour les cinq dernières années (2015 à 2019) concernant notamment le nombre de personnes physiques et morales enregistrées, leur nationalité et le nombre d'utilisateurs.

Deuxième examen de fonctionnement du Swiss-US Privacy Shield

En septembre 2019, le deuxième examen du bouclier de protection des données Suisse-États-Unis (Swiss-US Privacy Shield) a eu lieu à Washington D.C. Cette rencontre, qui s'est tenue tout juste après le troisième examen de l'accord sur le bouclier de protection Union européenne-États-Unis, a révélé de nouveaux progrès, mais aussi un potentiel d'amélioration.

Depuis l'entrée en vigueur en 2017 de l'accord sur le bouclier de protection entre la Suisse et les États-Unis, plus de 3300 entreprises ont intégré le programme, avec près de 1'000 entreprises certifiées supplémentaires depuis l'examen précédent (cf. 26e Rapport, ch. 1.2). À plus de 70 %, il s'agit de PME, mais les grands groupes tels que Facebook Inc. et Google LLC sont aussi certifiés (cf. https://www.privacyshield.gov/list)

Au cours de l'année sous revue, le Préposé a reçu un dossier à transmettre au Département américain du commerce (Department of Commerce, DoC). Il s'agissait d'une fausse déclaration (false claim), c'est-à-dire d'une entreprise qui se faisait passer à tort pour certifiée. L'affaire a été résolue en coopération avec le DoC (cf. 26e Rapport, ch. 1.2).

En outre, une dizaine de plaintes fondées visant des entreprises certifiées ont été déposées auprès d'organismes privés indépendants, spécialisés dans le règlement extrajudiciaire des litiges. Depuis la mise en œuvre de l'accord, notre autorité n'a été saisie d'aucun cas concernant l'accès des autorités américaines aux données personnelles pour des raisons de sécurité nationale.

Depuis le premier examen annuel du bouclier de protection des données entre la Suisse et les États-Unis et le second examen du bouclier UE-États-Unis, le fonctionnement de l'accord a été amélioré. Ainsi, le Département américain du commerce procède à des examens plus systématiques des entreprises certifiées et, par exemple, effectue tous les mois des contrôles aléatoires pour déterminer si les entreprises respectent certains principes énoncés dans l'accord. En outre, la Commission fédérale du commerce (Federal Trade Commission, FTC), chargée de l'application des règles de l'accord, agit désormais de plus en plus souvent d'office.

Les nominations qui ont eu lieu au sein des comités de surveillance et d'arbitrage constituent également un progrès par rapport à l'année précédente. Ainsi un médiateur permanent et les deux derniers membres manquants du Privacy and Civil Liberties Oversight Board (Organe indépendant de contrôle de la protection de la sphère privée et des libertés individuelles, PCLOB) ont été nommés.

Cependant, il reste encore des points à améliorer : tant pour le Préposé que pour le Comité européen de protection des données, la structure des compétences du médiateur n'est pas claire et le souhait d'une clarification a été exprimé. De même, les différends sur la question de savoir ce que recouvre exactement le terme de données relatives aux ressources humaines n'ont pas encore été éliminés.

Une certaine incertitude règne actuellement en raison d'un litige en cours devant la Cour de justice de l'Union européenne (CJUE) concernant le transfert de données entre l'UE et les États-Unis, qui pourrait avoir un impact sur le bouclier de protection UE-États-Unis. Même si les arrêts de la CJUE ne sont pas applicables à la Suisse, le Préposé devra analyser, compte tenu de la conception similaire des accords, si les considérants de la CJUE pourraient également être pertinents pour l'évaluation du bouclier de protection Suisse-États-Unis.

1.3 Fiscalité et finances

Communication de données personnelles à des autorités fiscales étrangères – extension problématique à d'autres États

La mise en œuvre des nouvelles normes visant à lutter, à l'échelle mondiale, contre la fraude et l'évasion fiscales a bien progressé. À cet égard, le niveau insuffisant de protection des données dans certains pays s'est avéré problématique. Au cours de l'année sous revue, nous avons pris position sur divers projets du point de vue de la protection des données.

Échange automatique de renseignements relatif aux comptes financiers (EAR)

La norme internationale régissant l'échange automatique de renseignements relatifs aux comptes financiers (EAR) est en vigueur en Suisse depuis le 1er janvier 2017. Elle vise à accroître la transparence dans le domaine fiscal afin de lutter contre la soustraction d'impôt sur le plan international. À ce jour, plus de 100 États, dont la Suisse, ont déclaré vouloir adopter cette norme.

Le réseau EAR de la Suisse doit être étendu à 18 États partenaires supplémentaires en vue d'une mise en œuvre de l'EAR à partir de 2020/2021, y compris à des pays comme le Ghana, le Kazakhstan, le Liban et le Nigeria. Comme pour les précédents élargissements de l'EAR à d'autres États, le Préposé a souligné à plusieurs reprises au cours de la période en cours la nécessité de garantir un niveau adéquat de protection des données dans l'État partenaire concerné. Si un tel niveau n'est pas garanti par les lois, la protection des données dans l'État partenaire doit être assurée par des garanties adéquates de protection des données (cf. art. 6, al. 2, LPD). Nous estimons cependant qu'aucune garantie suffisante n'a été créée dans le cadre de l'EAR (cf. 26e Rapport, ch. 1.3)

Dans le cadre de la consultation des offices sur le projet de modification de la loi fédérale sur l'échange international de renseignements en matière fiscale (LEAR), le Préposé s'est prononcé sur la nouvelle réglementation des compétences envisagée au cas où un État partenaire ne répondrait pas aux exigences de l'OCDE en matière de confidentialité et de sécurité des données. Il a proposé avec succès une nouvelle formulation précisant qu'en cas de non-respect des exigences de confidentialité et de sécurité des données, l'autorité suisse compétente a non seulement la possibilité mais l'obligation de suspendre, de sa propre autorité, l'EAR vis-à-vis de l'État partenaire. L'Assemblée fédérale n'a pas encore traité la proposition du Conseil fédéral au cours de l'année sous revue.

Échange de déclarations pays par pays (EDPP) des grands groupes multinationaux

Dès 2020, la Suisse échangera pour la première fois avec ses pays partenaires les rapports pays par pays des multinationales (cf. 24e Rapport, ch. 1.9.1). Au cours de l'année sous revue, le Préposé a exprimé son point de vue dans le cadre de la consultation des offices sur l'élargissement récemment prévu de la liste des pays partenaires pour l'activation de l'échange de déclarations pays par pays des entreprises multinationales. Il a souligné à ce propos que cet élargissement concernait les États et territoires figurant sur la liste des États dressée par le PFPDT avec un niveau de protection des données insuffisant (comme l'Arménie, la Bosnie et Herzégovine et les Îles Cook). Le Préposé a donc déclaré, comme il l'avait déjà fait lors de précédentes consultations d'offices, qu'en ce qui concerne ces pays, des garanties supplémentaires conformément à l'art. 6, al. 2, LPD sont nécessaires pour assurer un niveau adéquat de protection des données (cf. 26e Rapport, ch. 1.3).

Le Tribunal administratif fédéral admet le recours du Préposé dans l'affaire AFC : les tiers concernés ont droit à une information préalable

Le Tribunal administratif fédéral (TAF) a admis un recours du Préposé concernant le droit à l'information dans le cadre de l'assistance administrative en matière fiscale. La procédure de recours devant le Tribunal fédéral est provisoirement suspendue.

Fin décembre 2017, le Préposé a émis une recommandation formelle selon laquelle l'Administration fédérale des contributions (AFC) doit également informer au préalable, dans le cadre de l'assistance fiscale internationale, les personnes non concernées par la demande d'assistance administrative (à savoir les tiers) dont le nom doit être transmis en clair à l'autorité étrangère requérante, donc sous une forme non caviardée (cf. 25e Rapport, ch. 1.9.2). L'AFC a rejeté cette recommandation, à la suite de quoi le Préposé a d'abord soumis l'affaire au Département fédéral des finances (DFF), puis transmis la décision négative du DFF au Tribunal administratif fédéral (cf. 26e Rapport, ch. 1.3).

Dans son arrêt du 3 septembre 2019, le TAF est parvenu à la conclusion que, dans le cadre de l'assistance administrative en matière fiscale, les personnes non concernées par la demande d'assistance administrative (tierces personnes), dont les données sont transmises sous une forme non caviardée, doivent en principe être informées au préalable. Selon le Tribunal administratif fédéral, il faut élaborer des dispositions dérogatoires pour les cas où les informations requises impliqueraient un effort disproportionné et où l'exécution de l'assistance administrative serait impossible ou retardée de manière déraisonnable. Le Préposé se félicite de cet arrêt, car il protège les droits fondamentaux des employés de banque et autres tiers. En outre, il est prêt à travailler avec l'AFC pour trouver des solutions pratiques permettant de mettre en œuvre cet arrêt, ce qu'il a confirmé lors d'une réunion avec l'AFC à la fin de l'année 2019.

L'AFC a déposé un recours auprès du Tribunal fédéral. À la demande de l'AFC, la procédure a été suspendue car il est possible que l'arrêt en cette cause soit influencé par le jugement rendu dans un autre litige. Au cours de l'année sous revue, le Préposé n'a pas eu la possibilité de prendre connaissance de l'acte de recours adverse

.

1.4 Commerce et économie

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

Le Préposé a engagé une procédure d'éclaircissement des faits auprès d'une entreprise de premier plan dans le domaine du recouvrement, en raison d'écritures apparemment incorrectes.
Plusieurs questions de citoyens et comptes rendus dans les médias ont attiré l'attention du Préposé sur une entreprise offrant des informations de solvabilité et de crédit ainsi que des services de recouvrement. Il semblerait que des entrées incorrectes dans leur banque de données aient entraîné des méprises parmi des personnes ayant des noms ou adresses identiques ou similaires. De ce fait, des rappels de paiement auraient été envoyés à de mauvaises adresses ou des renseignements de solvabilité négatifs incorrects conservés et communiqués. Il a également été fait état de difficultés à corriger ces erreurs de saisies. En février 2020, afin d'enquêter sur ces critiques, le Préposé a ouvert une procédure d'établissement des faits. Elle était toujours en cours à la fin de l'année sous revue.

Utilisation des données de Ricardo au sein du groupe Tamedia (TX Group)

Le PFPDT a poursuivi son éclaircissement des faits relatif à l'utilisation des données collectées par la plateforme ricardo.ch, notamment au sein du groupe Tamedia (TX Group).
En juillet 2017, nous avions introduit une procédure d'éclaircissement des faits afin d'examiner la transparence et la conformité des traitements des données des utilisateurs et utilisatrices de la plateforme ricardo.ch au sein du groupe tamedia, ainsi que les possibilités de s'opposer notamment à l'exploitation des données à des fins de publicité ciblée (cf. 25e Rapport, ch. 1.8.8).

Depuis le début de la procédure, l'état de fait a sensiblement évolué ; entre autres, la déclaration de protection des données a été modifiée en mai 2018 avec l'entrée en vigueur du règlement européen de protection des données RGPD (cf. 26e Rapport, ch. 1.4.), puis en mars 2019 et en février 2020.

Tamedia AG (dans l'intervalle devenu TX Group AG) traite, analyse et agrège les données personnelles collectées sur la plateforme de commerce en ligne ricardo.ch notamment à des fins de marketing (publicité ciblée), de sorte que nous avons, dans le cadre de notre examen, étendu formellement la procédure à la société Tamedia AG. Nous avons soumis notre constatation des faits une nouvelle fois pour vérification et procédé à quelques adaptations. Notre évaluation juridique se basera sur les faits ainsi constatés

Adresses erronées chez Serafe AG – mesures nécessaires pour assurer l'exactitude des données

Au cours de l'année sous revue, l'entreprise Serafe AG a envoyé des milliers de factures erronées. L'entreprise a reconnu le problème et pris les premières mesures. Le Préposé examine si d'autres recommandations sont nécessaires du point de vue de la protection des données.

Depuis le début de l'année 2019, Serafe AG est le nouvel organisme suisse de recouvrement de la redevance radio-télévision. À la suite d'un appel d'offres public, le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) lui a confié un mandat valable jusqu'au 31 décembre 2025.

Selon des informations transmises au Préposé par des particuliers et divers comptes rendus parus dans les médias, Serafe AG a envoyé en janvier 2019 des milliers de factures mal adressées. Ainsi des factures ont été envoyées à des adresses qui ne sont plus valables, sont parvenues à de mauvais destinataires ou ont été émises plusieurs fois au nom d'un même destinataire. Les données des ménages, nécessaires à la perception de la redevance, auraient été fournies par les cantons et les communes à partir des registres du contrôle des habitants ; or certaines de ces données étaient inexactes. Les problème auraient été reconnus et des mesures prises afin de garantir l'exactitude des données à l'avenir.

Le Préposé a prié Serafe AG de s'expliquer. Sur la base de sa réponse, il examinera s'il doit procéder à une clarification de la situation en vertu de la législation sur la protection des données et, le cas échéant, recommander d'autres mesures aux responsables afin de garantir un traitement des données conforme à la loi

.

Analyse des données de transaction à des fins de planification

Une enseigne commerciale a sollicité l'avis du PFPDT concernant l'exploitation de données de transaction de sa clientèle à des finalités ne se rapportant pas à des personnes. Dans le cadre de nos compétences de conseil, nous avons examiné et évalué le projet tant sous un angle technique que juridique.

L'enseigne commerciale, active dans le commerce de détail et disposant de plusieurs magasins en Suisse, nous a présenté son projet d'exploiter les données de transaction de sa clientèle à des finalités ne se rapportant pas à des personnes, dans le cadre de la planification commerciale.

Selon le concept présenté, il s'agissait, d'une part, d'utiliser les données collectées par l'enseigne au moment de la transaction, et d'autre part, les données saisies par le fournisseur de service de paiement,. La combinaison des données disponibles de part et d'autre permettrait de suivre les transactions effectuées à partir d'une certaine carte de paiement et d'établir un profil de consommation sur la durée (profil transversal), ce que l'enseigne n'est pas en mesure de faire avec les seules données dont elle dispose. L'enseigne précisait toutefois qu'une telle analyse serait effectuée exclusivement à des fins ne se rapportant pas à des personnes (en particulier pas de publicité ciblée).

L'enseigne commerciale ne saisissant pas les données concernant la carte de paiement, le fournisseur de service de paiement devrait transmettre au préalable ces données. Pour ce faire, le concept prévoyait de remplacer le numéro de la carte de paiement par un identifiant unique (« token »), générée au terme d'un processus de hachage (pseudonymisation).

Au terme d'une évaluation technique et juridique des documents fournis, effectuée dans le cadre de notre activité de conseil, nous avons conclu que tant le traitement des données effectué par le fournisseur de service de paiement que celui effectué par l'enseigne étaient soumis à la LPD, les données traitées de part et d'autre étant bel et bien des données personnelles. L'attribution d'un identifiant unique (effectuée grâce à la fonction de hachage) rend les données plus difficilement identifiables et permet de minimiser l'atteinte à la personnalité, cela conformément aux principes de proportionnalité et de sécurité. Les autres principes généraux de protection des données, tels que le principe de finalité et de transparence, sont également applicables.

La communication des données par le fournisseur de service de paiement représente un changement de finalité par rapport au traitement de données initial (qui est d'assurer le service de paiement) ; un tel changement de finalité doit être légitimé par un motif justificatif, dans le cas particulier le consentement libre et éclairé du client concerné. Sur le plan des mesures techniques, nous avons souligné qu'il fallait utiliser une fonction de hachage avec salage ou clé secrète, à des fins de sécurité.

Quant à l'enseigne commerciale, nous avons estimé que celle-ci pourrait invoquer l'intérêt privé prépondérant prévu par l'article 13 al. 2 lit. e LPD, pour autant qu'elle s'en tienne aux conditions énoncées : les données personnelles doivent être traitées à des fins ne se rapportant pas à des personnes, dans le cadre de la recherche, de la planification ou de la statistique ; de plus, les résultats doivent être publiés sous une forme ne permettant pas d'identifier les personnes concernées. Dans le cas particulier, cela signifie que les connaissances obtenues par les analyses de profils ne peuvent pas – sur la base de ce motif justificatif – être utilisées pour la publicité ciblée et que l'enseigne commerciale ne peut pas les combiner avec d'autres données personnelles dont elle disposerait (carte de fidélité, e-shop ou autre). Dans le cas contraire, une telle utilisation nécessiterait le consentement explicite des personnes concernées, compte tenu du profilage effectué.

L'enseigne commerciale a accusé bonne réception de notre évaluation et nous informera en cas de mise en œuvre du projet.

L'enseigne de sport Décathlon a informé de manière lacunaire sur sa collecte de données

Dans le cadre d'un procédure d'établissement des faits, le Préposé a demandé à Décathlon de mieux informer ses clients sur sa politique de collecte des données. Le détaillant d'articles de sport a remanié sa déclaration de protection des données.

En 2018, nous avons introduit une procédure d'établissement des faits chez le détaillant d'articles de sport Décathlon après avoir appris de diverses sources qu'il subordonnait la vente de marchandises dans ses magasins suisses à la fourniture de certaines données de clients. À la suite de l'ouverture de la procédure, Décathlon a informé le Préposé que les clients devaient fournir leur adresse électronique ou leur numéro de téléphone afin de pouvoir acheter des marchandises en magasin. Le détaillant a toutefois ajouté qu'il s'abstiendrait à l'avenir de faire dépendre la vente de biens de la fourniture de ces données et ne recueillerait désormais ces données que sur une base volontaire. Le Préposé s'est alors penché sur la question de savoir si le caractère volontaire de la collecte de données était manifeste pour les clients et si ceux-ci étaient suffisamment informés. Il a proposé des modifications à la grande enseigne sportive afin d'améliorer l'information des clients (cf. 26e Rapport, ch. 1.4). Décathlon a tenu compte de toutes les suggestions du Préposé et a achevé la révision de sa déclaration de protection des données.

Authentification par reconnaissance vocale chez PostFinance SA

PostFinance SA s'est adressée au Préposé et lui a présenté son projet de reconnaissance vocale dans son centre de contact. Le Préposé a fait remarquer à l'entreprise que les empreintes vocales en tant que données biométriques relatives à des personnes comportaient un risque accru et devraient donc être particulièrement protégées.

Au cours de l'année sous revue, PostFinance SA a présenté au Préposé un projet visant à identifier par leur voix les clients appelant son centre de contact. L'identité de l'appelant est vérifiée par comparaison avec une empreinte vocale enregistrée. PostFinance SA a précisé que les empreintes vocales enregistrées ne seraient utilisées que pour authentifier les clients au téléphone et qu'actuellement, elle ne prévoyait pas d'utiliser ces données pour d'autres analyses plus approfondies.

Contrairement au règlement général de l'UE sur la protection des données (RGPD), la loi suisse sur la protection des données ne mentionne pas les données biométriques parmi les données sensibles – même si leur traitement comporte des risques particuliers. Les caractéristiques biométriques sont intrinsèquement liées à une personne spécifique et, contrairement aux mots de passe, ne peuvent pas être remplacées après une panne ou une utilisation abusive. En raison des progrès techniques accomplis par les programmes de reconnaissance vocale et faciale (cf. ch. 1.1, article Clearview) ainsi que des risques accrus pour les droits de la personnalité auxquels sont exposées les personnes concernées, le traitement des données biométriques basé sur ces technologies doit garantir une protection accrue en droit de la protection des données. Dans les cas où il est nécessaire de recueillir un consentement en vertu de la LPD, le Préposé estime qu'il faut expressément le demander avant la collecte des données. Le maître du fichier doit également fournir à l'avance des informations détaillées et transparentes sur le traitement des données.

Dans le cadre de ses tâches de conseil, le Préposé a enjoint PostFinance SA d'adopter ce type de mesures. L'entreprise a tout d'abord obtempéré. Mais, plus tard, elle a modifié son comportement et depuis lors, n'a accordé à ses clients suisses qu'une option de retrait (opt-out) : donc pour que la reconnaissance vocale ne soit pas utilisée dans leur cas, ils doivent signifier explicitement leur refus.

Nous avons demandé à PostFinance SA une prise de position écrite, d'autant plus que nous avons constaté que les clients étrangers ne seront soumis à la reconnaissance vocale qu'après avoir donné explicitement leur accord, c'est-à-dire par le biais de l'opt-in. Dans sa prise de position, PostFinance SA a confirmé qu'elle avait modifié le processus fin 2018 après avoir recueilli l'avis d'une partie tierce dans le cadre d'un nouvel examen de la conformité juridique. Selon PostFinance, les clients suisses seraient informés de l'enregistrement de leur empreinte vocale par une annonce automatique. Les clients ne souhaitant pas l'établissement de leur empreinte vocale devraient devenir eux-mêmes actifs et informer leur conseiller à la clientèle de leur refus ou désactiver ultérieurement la fonction sur leur portail e-finance. Pour ce qui est de la clientèle étrangère, PostFinance SA estime qu'il ne peut être exclu que des règles plus strictes en matière de protection des données soient appliquées, en particulier celles du RGPD, raison pour laquelle un consentement préalable explicite continuerait à leur être demandé.

Le Préposé a pris note des explications de PostFinance SA et a publiquement souligné la nécessité de relever, dans un avenir proche, le niveau de protection des données concernant la population suisse. Tant que la révision totale de la LPD n'entrera pas en vigueur (voir Accent I), les clients domiciliés en Suisse devront s'attendre à ce que les entreprises suisses leur réservent un traitement plus défavorable qu'aux clients domiciliés à l'étranger.

Migros : vidéosurveillance par caméras intelligentes

Au cours de l'année sous revue, Migros a introduit à titre d'essai un nouveau système de caméras de surveillance dans ses magasins. Le Préposé en vérifie la conformité au droit de la protection des données.

Le Préposé a appris par la presse que l'entreprise Migros utilisait de nouveaux types de caméras de surveillance. Interrogée, Migros a confirmé qu'elle testait un nouveau système à titre de projet-pilote dans quelques-unes de ses filiales. En cas d'incident , le logiciel utilisé permet d'analyser les clients en fonction de certains critères d'apparence et d'identifier les séquences vidéo pertinentes. Les nouvelles caméras ne seront toutefois pas utilisées pour la reconnaissance faciale.

De l'avis du Préposé, plusieurs questions se posent pour que ce type de système soit, dans sa conception, conforme aux principes de protection des données. La transparence à l'égard des personnes concernées et la garantie de normes de sécurité élevées pendant le traitement des données revêtent une importance cruciale. Suite à ses premières clarifications, le Préposé a ouvert une procédure d'établissement des faits afin d'examiner le système de manière approfondie et, si nécessaire, d'émettre des recommandations en matière de protection des données. Cette procédure était toujours en cours à la fin de l'année sous revue.

1.5 Santé

Intensification des contacts dans la perspective de l'introduction du dossier électronique du patient

À partir du 15 avril 2020, le dossier électronique du patient (DEP) sera mis à la disposition des citoyens dans toute la Suisse. Compte tenu de cette introduction imminente, le Préposé s'est à nouveau penché sur cette thématique au cours de l'année sous revue – en particulier à propos des prestataires, à savoir les communautés de référence.

Avec le DEP, les particuliers disposeront, sous forme numérisée, de leurs données personnelles de santé telles que les maladies ou les médicaments qui leur sont prescrits, et décideront eux-mêmes qui peut les consulter. Le projet d'introduire en date du 15 avril 2020 le dossier électronique du patient a provoqué une nouvelle augmentation du nombre de demandes de renseignements adressées au Préposé par les citoyens. Nous avons également intensifié nos efforts de coordination avec les préposés cantonaux à la protection des données et participé à diverses rencontres de spécialistes.

En raison de l'importance et de l'actualité du sujet, le Préposé a en outre obtenu des informations de première main de l'une des plus grandes communautés de référence en Suisse, sur l'état des travaux, la mise en œuvre et les difficultés d'introduction du DEP. Selon la loi, ces organismes sont les seuls habilités à offrir le DEP et sont placés sous la surveillance du Préposé, tandis que les institutions pour la plupart cantonales comme les hôpitaux sont supervisées par les préposés cantonaux à la protection des données. Le Préposé a ainsi obtenu une vue d'ensemble des travaux de développement et des opérations et instruments techniques complexes et nécessaires au fonctionnement du DEP. Il est apparu à cet égard que non seulement la structuration des communautés de référence est difficile du point de vue technique, mais aussi que le processus de certification implique un volume important de démarches à la charge des communautés de référence et des éditeurs de moyens d'identification de l'identité électronique dans le DEP.

Selon les informations fournies par les organismes compétents, la phase de déploiement du DEP se poursuivra jusqu'à l'été 2020. Le Préposé continuera à en suivre l'évolution et envisagera de procéder à des contrôles dès que les communautés de référence auront entamé leurs activités.

Programme de bonus Helsana+ – mise en œuvre de l'arrêt du Tribunal administratif fédéral

En 2019, le Tribunal administratif fédéral (TAF) avait considéré comme illicites certains traitements de données effectués par l'assureur dans le cadre du programme de bonus Helsana+. Au cours de l'année sous revue, le Préposé a contacté Helsana à diverses reprises afin de s'assurer que l'arrêt du TAF était pleinement appliqué et que les futures adaptations des dispositions d'utilisation répondraient également aux exigences légales de la protection des données.

Dans son arrêt du 19 mars 2019, le TAF a qualifié d'illicite la collecte de données auprès de l'assurance de base sous sa forme initiale en l'absence de consentement juridiquement valable (cf. 26e Rapport, ch. 1.5). Dans ses considérants, le tribunal a constaté, dans les dispositions d'utilisation et de protection des données d'Helsana+, certaines lacunes qui, de l'avis du Préposé, existent indépendamment de la question du consentement valable.

Après l'entrée en vigueur de cet arrêt, le Préposé a donc exigé qu'Helsana remédie aux lacunes constatées dans les dispositions d'utilisation et de protection des données de Helsana+ afin que ces dispositions répondent aux critères de transparence et de compréhensibilité.

Dans l'intervalle, l'assureur a révisé en profondeur les conditions d'utilisation du programme de bonus. En ce qui concerne plus particulièrement les nouvelles règles, le Préposé demeure en contact avec l'assureur afin de garantir que les traitements de données sont bien effectués dans le respect des règles de protection des données.

« Swiss National Cohort » : des précautions supplémentaires sont nécessaires

Le projet de recherche « Swiss National Cohort » (SNC) a pris de l'ampleur et donne désormais lieu à des appariements tels que les données traitées ne sont plus anonymes : un renforcement du dispositif de confidentialité s'impose.

En partenariat avec l'Office fédéral de la statistique (OFS), l'Institut pour l'épidémiologie, la biostatistique et la prévention (EBPI) de l'Université de Zürich et l'Institut pour la médecine sociale et préventive (ISPM) de l'Université de Berne se sont associés pour créer dès 2006 la première cohorte représentant l'ensemble de la population suisse, à long terme, et constituer ainsi une plateforme de recherche polyvalente. Donnant suite aux sollicitations de l'ISPM, nous avons pris position quant au respect de la protection des données par la SNC, dans le respect et sous réserve des compétences des préposés cantonaux à la protection des données concernés.

Nous avons ainsi constaté que les mesures techniques et organisationnelles étaient aptes à garantir la sécurité et l'exactitude des données. En revanche, contrairement aux phases précédentes du projet, nous avons remarqué que de nombreuses données personnelles, y compris des données de santé, étaient désormais appariées, rendant toute anonymisation impossible. Nous avons donc recommandé aux promoteurs du projet de prendre des précautions supplémentaires afin de garantir la confidentialité des données des personnes concernées.

IQOS : Enquête sur la cigarette électronique nouvelle génération IQOS auprès de Philip Morris

Les cigarettes électroniques IQOS de Philip Morris n'engendrent ni feu ni cendres, mais d'abondantes données. Le Préposé a examiné si leur gestion respecte la protection des données.

Alors que le marché des cigarettes électroniques progresse et que le Parlement élabore en ce moment une loi sur les produits du tabac et les cigarettes électroniques (LPTab), l'entreprise Philip Morris a ces dernières années développé un nouveau produit : composée de bâtonnets de tabac appelés « heets » et d'un appareil qui les chauffe sans les brûler, IQOS comporte aussi une connexion bluetooth qui permet d'exporter les données du système.

Plus qu'une cigarette électronique, IQOS est donc aussi un objet connecté. Plusieurs articles de presse ayant évoqué des craintes quant à la protection des données issues d'IQOS, le Préposé a ouvert le 11 juillet 2019 une procédure d'établissement des faits afin de déterminer si les traitements de données réalisés en lien avec IQOS sont susceptibles de porter atteinte à la sphère privée des consommateurs en Suisse.

L'observation des prescriptions légales en matière d'information, de consentement et de communication transfrontière des données, tant à l'intérieur qu'à l'extérieur de la multinationale, ont été au centre de son enquête, qui a permis de s'assurer que les mesures techniques et organisationnelles prises par Philip Morris étaient aptes à garantir la protection des données personnelles des utilisateurs en Suisse.

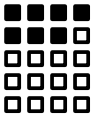
1.6 Secteur du travail

Applications ciblées sur le traçage et la saisie du temps dans l'espace de travail

Les téléphones intelligents sont de plus en plus utilisés à des fins professionnelles, par exemple lorsqu'ils disposent d'applications permettant de saisir les heures de travail ou les trajets effectués pendant celles-ci. Pour être conforme aux principes de la protection des données, ce type d'application doit limiter le traitement des données au strict nécessaire et les employés doivent être informés de manière appropriée.

Au cours de l'année sous revue, nous avons constaté une recrudescence des demandes du public concernant l'utilisation des applications mobiles dans le domaine du travail. Saisie du temps, traçage par GPS, accès aux e-mails professionnels – il n'y a guère de domaines de la vie professionnelle qui ne puissent être traités également par téléphone portable.

Avoir son bureau dans la poche simplifie certes la vie professionnelle au jour le jour, mais pose également un certain nombre de questions juridiques touchant à la protection des données, d'autant plus que bon nombre de ces fonctions techniques peuvent aussi être utilisées pour surveiller les employés.



Une utilisation conforme à la protection des données des applications mobiles dans le domaine du travail exige que l'employeur traite uniquement les données personnelles de ses collaborateurs qui sont nécessaires à l'exécution du contrat de travail. En outre, les principes de traitement de la LPD tels que la proportionnalité et la transparence doivent toujours être respectés. Quant à ce dernier point en particulier, nous observons des lacunes car souvent, les employés ne sont pas suffisamment informés de l'utilisation ou de l'objectif des mesures de surveillance.

Un autre sujet délicat est celui des mesures techniques et organisationnelles qui devraient empêcher l'utilisation abusive des données et leur accès par des personnes non autorisées, même au sein de l'entreprise.

Dans bien des cas enfin, le flou règne sur l'utilisation des données du traçage par GPS pendant les pauses ou une fois la journée de travail terminée, ce type de traitements de données constituant en principe une violation de la sphère privée des collaborateurs. De ce fait, nombreuses ont été les personnes concernées à nous demander conseil à ce propos.

Les problèmes liés aux fonctions mobiles de la vie professionnelle sont encore aggravés lorsque le même smartphone est utilisé à des fins privées et professionnelles. Dans ce cas précis, la question qui se pose est de savoir comment procéder correctement à la fin de la relation de travail.

Le Préposé continue de suivre avec attention les développements en matière d'applications mobiles dans la vie professionnelle et a également ouvert une procédure d'établissement des faits à ce sujet (voir encadré).

Établissement des faits en matière de saisie du temps

Le Préposé a ouvert une procédure d'établissement des faits auprès d'une grande entreprise spécialisée dans le nettoyage et l'entretien des bâtiments. Cette entreprise emploie un nombre important de personnes et, depuis peu, a numérisé en grande partie son système de saisie du temps. L'enregistrement des heures de travail, désormais basé sur Internet, soulève un certain nombre de questions relatives à la protection des données, notamment quant à la sécurité des données, aux règles d'accès et aux flux de données au sein de l'entreprise et vers des tiers éventuels. Le Préposé informera du résultat de ses démarches à la fin de la procédure.

Utilisation de l'intelligence artificielle dans le recrutement

De plus en plus souvent, l'intelligence artificielle est utilisée dans les processus de recrutement. Fréquemment, l'atteinte aux droits individuels est alors plus grave que dans les processus de candidature classiques.

Plusieurs comptes rendus des médias et questions de citoyens au cours de l'année sous revue laissent penser qu'en Suisse aussi, l'intelligence artificielle (IA) est de plus en plus utilisée dans les processus de candidature. Les entretiens d'embauche sont par exemple enregistrés sur vidéo, puis analysés par un logiciel.

Tout d'abord, le cadre de protection des données applicable à la mise en œuvre de ces nouveaux instruments est le même que pour les procédures de recrutement classiques : l'employeur ne peut collecter et traiter que les données nécessaires pour clarifier l'aptitude d'une personne à occuper le poste en question et doit toujours respecter les principes figurant dans la législation sur la protection des données.

Par ailleurs, compte tenu de la richesse des possibilités d'analyse offertes par les processus s'appuyant sur l'intelligence artificielle, les atteintes aux droits de la personnalité ont tendance à y être plus graves que dans les entretiens d'embauche menés de manière conventionnelle. Le principe de reconnaissabilité et de proportionnalité requièrent de ce fait une attention toute particulière.

Selon les renseignements fournis par l'Office fédéral du personnel (OFPER), actuellement la Confédération n'utilise pas l'intelligence artificielle dans ses procédures de recrutement. Si cela devait être le cas à l'avenir, le Préposé interviendrait à un stade précoce et exigerait que l'utilisation des technologies en question soit modérée et conforme à la protection des données

.

1.7 Assurances

Entrée en vigueur de nouvelles dispositions légales sur les observations dans le domaine des assurances sociales

Les nouvelles bases légales pour la surveillance des assurés ont été intégrées dans la loi fédérale sur la partie générale du droit des assurances sociales (LPGA) et sont entrées en vigueur le 1er octobre 2019, en même temps que les dispositions de l'ordonnance y relative. Au cours de l'année sous revue, nous avons conseillé les citoyens qui nous ont contactés pour obtenir des conseils juridiques en matière de surveillance.

Au cours de l'année sous revue, la surveillance dans le secteur des assurances sociales a été réorganisée sur la base de l'article relatif à l'observation. Les bases légales requises sont entrées en vigueur le 1er octobre 2019 avec les art. 43a et 43b de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA) et les dispositions d'exécution figurant dans l'ordonnance y relative aux art. 7a à 9b OPGA. Celles-ci régissent les conditions et les moyens autorisés pour l'observation secrète des personnes assurées soupçonnées de fraude à l'assurance.

L'adoption de dispositions légales dans ce domaine était devenue nécessaire à la suite de l'arrêt « Vukota-Bojic c. Suisse » rendu le 18 octobre 2016 par la Cour européenne des droits de l'homme (CEDH) de Strasbourg (requête n° 61838/10), selon lequel la Suisse ne disposait pas de base légale suffisante lui permettant de recourir à des détectives privés dans le domaine des assurances sociales. De l'avis de la CEDH, les mesures de surveillance ordonnées par l'assureur avaient donc violé le droit à la vie privée, protégé par l'article 8 de la Convention européenne des droits de l'homme.

Le Préposé considérant que la protection de la sphère privée était considérablement affectée par ce type d'observations, il a participé très tôt au processus législatif. Il a notamment requis qu'une observation ne puisse être ordonnée que par une personne assumant une fonction de direction dans le domaine dont relève le cas à traiter ou dans le domaine des prestations de l'assureur. Il a également demandé que la durée de la surveillance soit limitée par la loi. Ces deux aspects ont été intégrés à l'art. 43a LPGA. Avant cette modification de loi, les détectives privés ne pouvaient être employés à des fins d'observation que dans le cadre de l'assurance-invalidité (AI) et de l'assurance-accidents (AA).

Désormais, les observations sont également possibles dans les autres branches des assurances sociales : assurance-chômage, assurance-maladie obligatoire, assurance militaire, prestations complémentaires, régime des allocations pour perte de gain et AVS. Comme certaines de ces assurances sont gérées par des services cantonaux, qui peuvent en conséquence ordonner des observations, les activités de surveillance dans ces domaines sont supervisées par les préposés cantonaux à la protection des données. Le Préposé fédéral est quant à lui chargé de la surveillance et des conseils en matière de protection des données dans les domaines de l'assurance-accidents, de l'assurance-maladie obligatoire et de l'assurance militaire ; les observations ordonnées dans le cadre de ces assurances sociales relèvent donc également de sa compétence.

Projet de loi concernant l'utilisation systématique du numéro AVS

Le 30 septembre 2019, le Conseil fédéral a transmis au Parlement un message relatif à une modification de la loi fédérale sur l'assurance-vieillesse et survivants. Le projet prévoit d'autoriser les administrations fédérales, cantonales et communales à utiliser systématiquement le numéro AVS comme identifiant unique en dehors du domaine des assurances sociales.
Le projet met un point final à un long processus qui a conduit le législateur fédéral à étendre l'utilisation du numéro AVS bien au-delà du domaine des assurances sociales par le biais de nombreuses lois spéciales. Ces extensions ont notamment été discutées lors de l'examen de la modernisation du droit du registre du commerce et du droit du registre foncier, auquel les Commissions des affaires juridiques des deux Conseils ont associé le Préposé. Dans ce contexte, nous avons convaincu l'Office fédéral de la justice (OFJ) de commander avec nous une étude sur les risques, du point de vue de la protection des données, à l'EPF de Zurich et d'intégrer les résultats de celle-ci dans l'examen de la modernisation du droit du registre foncier. L'étude a clairement mis en évidence que les registres de personnes de la Confédération, des cantons et des communes sont exposés aux accès non autorisés et abusifs. L'expert a également démontré que l'utilisation d'identifiants sectoriels, tels que prévus par la législation fédérale notamment pour la gestion du dossier électronique du patient, ne permettait pas à elle seule de réduire significativement les risques en matière de protection des données. Après avoir pris acte des résultats de l'étude, la Commission des affaires juridiques du Conseil national a chargé le Conseil fédéral, en 2017, de montrer dans un concept comment il est possible de minimiser les risques mis en évidence par l'étude et de prendre pour cela en considération l'avis du Préposé (cf. 25e Rapport, ch. 1.1.2).

Le Conseil fédéral s'est acquitté de son mandat dans le cadre du message précité, à l'élaboration duquel nous avons été étroitement associés par l'Office fédéral des assurances sociales (OFAS) ainsi qu'à celle du projet de loi. Nos propositions et nos observations ont été prises en considération. Compte tenu des risques sérieux pour la protection des données, nous saluons le fait que le projet de loi prévoit expressément l'obligation pour les entités disposant de banques de données dans lesquelles le numéro AVS est utilisé de manière systématique de procéder périodiquement à des analyses de risques, en tenant compte notamment du danger d'appariements non autorisés de données. Sur la base de cette analyse de risques, il convient de définir et de mettre en œuvre des mesures de sécurité et de protection des données qui soient adaptées à la situation de risque et correspondent à l'état de la technique. Nous saluons également l'obligation pour les entités désignées par le projet de loi utilisant systématiquement le numéro AVS de tenir un registre des banques de données pertinentes servant en particulier de base aux analyses de risques à effectuer. Le Préposé se félicite en outre de la promesse du Conseil fédéral, en vertu de laquelle l'utilisation systématique du numéro AVS ne conduira pas à ce que l'administration outrepasse les compétences qui sont les siennes dans un État de droit. Nous veillerons à ce que l'administration fédérale respecte cette promesse. Le Conseil fédéral confirme par ailleurs que l'utilisation systématique du numéro AVS ne fera pas du numéro de sécurité sociale un identifiant unique, comme aux États-Unis ou en Scandinavie où les cas d'usurpation d'identité se sont multipliés. Pour prévenir ce risque, l'utilisation du numéro AVS par des particuliers sera limitée. La loi prévoit en outre que les personnes habilitées à accéder aux données seront informés, dans le cadre de formations et de perfectionnements, que le numéro AVS ne peut être utilisé qu'en rapport avec leurs tâches. Le Préposé se félicite du fait qu'il sera également possible dans le cadre de la modification de la LAVS de recourir à l'identification électronique, au moyen d'un numéro d'enregistrement e-ID, indépendant du numéro AVS, afin de favorise la sécurité de l'échange de données entre les particuliers et les autorités.

Les mesures techniques du projet de loi sont également importantes car elles exigent entre autres que les fichiers de données comprenant le numéro AVS ne transitent plus à l'avenir que sous forme cryptée via le réseau public.

Appelé à se prononcer devant la Commission des institutions politiques du Conseil des Etats lors de sa séance du 18 février 2020, le Préposé a pu rappeler l'importance des garanties et mesures concrètes pour réduire les risques au maximum ainsi que, dans ce contexte, la nécessité pour la Confédération, les cantons et les communes, de revoir progressivement la conception de l'architecture de leurs banques de données

1.8 Transports

L'application de transports publics SmartWay crée des profils de de la personnalité

L'offre d'applications en matière de transports publics ne cesse d'augmenter. Dans ce contexte, le Préposé a conseillé les CFF qui, au cours de l'année écoulée, ont lancé deux applications de mobilité, EasyRide, pour la billetterie électronique et SmartWay, un assistant de voyage électronique.

Face à l'offre croissante d'applications de mobilité, le Préposé a déjà conseillé diverses entreprises de transport au cours des dernières années, notamment en matière de billetterie électronique (cf. 24e Rapport, ch. 1.2.4). Au cours de l'année sous revue, le Préposé a poursuivi l'échange avec plusieurs entreprises de transport, en particulier avec le conseiller à la protection des données des CFF, entre autres sur la technologie Fairtiq pour la billetterie électronique. Le Préposé a notamment contribué à ce que les conditions d'utilisation du système EasyRide, basé auprès de Fairtiq, soient plus conviviales et proportionnées. En outre, il a demandé qu'il lui soit garanti que les restrictions relatives à la communication et au traitement ultérieur des données par des tiers seront effectivement respectées.

Les CFF ont également présenté au Préposé l'application Smartway, une application très gourmande en données et encore en phase de test. Elle fournit aux utilisateurs des recommandations de voyage personnalisées, accompagnées des correspondances appropriées. Qu'elle soit utilisée au non, avec l'application Smartway, les données sont enregistrées en continu 24h sur 24 et les utilisateurs ne peuvent pas refuser cette fonction. Or, s'ils ne les suppriment pas de manière active ou n'utilisent pas l'application pendant plusieurs mois, les données recueillies ne sont effacées qu'au bout de quatre ans.

Quelques jours d'utilisation suffisent pour créer des profils de personnalité et il est pratiquement impossible d'anonymiser les profils de déplacement. Par conséquent, des exigences très élevées doivent être posées eu égard à la protection des données, notamment quant à la proportionnalité et à l'information. Le Préposé a souligné que les utilisateurs, avant de s'enregistrer, doivent être informés de manière complète et compréhensible à propos de tous les traitements concernant leurs données personnelles, cela afin de pouvoir donner leur consentement de façon libre et éclairée. Il faut qu'ils sachent clairement qui traite quelles données et dans quel but. De plus, leur consentement doit être donné de manière explicite (opt-in), en fonction de l'objectif poursuivi et non pas de manière générale. La transparence doit être de mise sur la manière dont le droit d'accès – également en cas de traitement des données confié par mandat à des tiers – peut être exercé et sur la question de savoir si les profils sont également supprimés auprès de tiers lorsqu'ils sont effacés dans l'application. Dans la négative, les utilisateurs doivent être clairement informés de la manière dont ils peuvent supprimer les données dans leur totalité. Si des données sont traitées à l'étranger, par exemple dans un nuage, les utilisateurs doivent en être informés de manière adéquate, avec mention du pays pour les demandes d'accès et d'effacement. D'une manière générale, les tiers qui traitent des données personnelles se doivent aussi de respecter les principes de protection et de sécurité des données.

Le Préposé a rappelé que les tiers qui traitent des données personnelles sont chargés de garantir la protection des données depuis le début et de procéder en permanence à des analyses de risques au cours du développement du projet.

Contrôle d'un projet-pilote des CFF et d'Axon Vibe

À la suite d'une longue interruption de la liaison ferroviaire entre Lausanne et Puidoux-Chexbres, les CFF ont lancé un projet-pilote afin d'indemniser les clients. Le Préposé a ouvert une procédure d'établissement des faits concernant le traitement correct des données.

En été 2018, les CFF ont été obligés de fermer pendant plusieurs mois la liaison ferroviaire entre Lausanne et Puidoux-Chexbres en raison de travaux. Désireux d'offrir une compensation équitable à ses clients incommodés à diverses reprises par des retards importants, les CFF ont alors lancé un projet-pilote. Ainsi, les trajets accomplis par les clients CFF participant au projet-pilote de compensation ont été automatiquement enregistrés via les fonctions « Géolocalisation » et « Mouvement et forme » de leur Smartphone. Cela a permis, entre autres, de traiter les données relatives à leurs déplacements. Comme cela soulève également des questions juridiques touchant à la protection des données, le Préposé a décidé de procéder à un établissement des faits à propos du traitement de ces données personnelles.

Pour notre autorité, le but de cette inspection était de vérifier si les CFF traitait les données personnelles conformément à la loi, ainsi qu'ils s'y étaient engagés. Nous désirions tout particulièrement examiner l'utilisation exclusive des données personnelles pour ce projet-pilote ainsi que l'effacement des données. Nous nous sommes également concentrés sur le transfert de données des CFF à Axon Vibe et leur traitement ultérieur par cette société tierce.

Au cours de notre examen des faits, il est apparu clairement que divers aspects pertinents en droit de la protection des données allaient au-delà des nécessités du projet-pilote. Par exemple, les données utiles au projet-pilote avaient été collectées par un système plus étendu (travel cockpit) d'Axon Vibe, qui contenait déjà d'autres données de clients. Il n'y avait pas de séparation nette entre ces données et les données collectées dans le cadre du projet-pilote.

Par ailleurs encore, il était difficile de déterminer qui était le responsable du traitement des données, les CFF ou Axon Vibe.

Une analyse détaillée aurait nécessité une nouvelle procédure approfondie d'établissement des faits. Le projet-pilote était si très étroitement défini en temps et en lieu que relativement peu de clients ont été touchés. De plus, les CFF ont entre-temps lancé des applications nécessitant une masse beaucoup plus grande de données sur lesquelles le Préposé se concentre actuellement ; il s'est donc limité à vérifier la suppression correcte et définitive de toutes les données personnelles rassemblées dans le cadre du projet-pilote en question.

Notre échange de courrier avec les CFF et Axon Vibe était toujours en cours à la fin de l'année sous revue.

Protection de la sphère privée dans le cadre du projet de tarification de la mobilité

Dans la perspective d'une augmentation de la population suisse à 10 millions d'habitants, l'Office fédéral des routes (OFROU) planifie une régulation du comportement de la population en matière de mobilité par le biais des frais de déplacement. Cette tarification de la mobilité (Mobility Pricing) devrait dépendre du moment de la journée, de la distance parcourue et du moyen de transport utilisé. Ce projet est en phase initiale. Le Préposé demande que les exigences posées par la législation sur la protection des données soient intégrées le plus tôt possible au processus.

Selon l'Office fédéral des routes, l'augmentation de la population estimée à dix millions d'ici une vingtaine d'années en Suisse serait une surcharge pour l'ensemble du système de transport actuel. Face à l'impossibilité de développer les infrastructures traditionnelles dans la mesure requise et de mettre en place rapidement des systèmes visionnaires tels que les structures souterraines, l'OFROU entend se concentrer sur des solutions à même d'influer sur le comportement des Suisses en matière de mobilité, ceci afin de réduire les pics d'affluence. La tarification de la mobilité consiste à faire payer les usagers en fonction de la distance parcourue sur le territoire suisse, selon le moment de la journée et le moyen de transport utilisé.

La mise en œuvre de la tarification de la mobilité nécessite la saisie du comportement des usagers et donc le traitement de données personnelles et de profils de déplacement dans certains cas sensibles (cf. supra).

Pour l'heure, le Préposé estime possible de concevoir la tarification de la mobilité dans le respect des règles de protection des données. Au cours de l'année sous revue, lors de plusieurs réunions avec l'OFROU et dans ses observations écrites, le Préposé a œuvré pour que la protection des données soit reconnue et intégrée très tôt au projet. Nous attachons une importance particulière à ce que tous les acteurs du secteur public et du secteur privé participant au projet disposent

d'un conseiller interne à la protection des données doté de ressources suffisantes. Ces conseillers doivent être associés au projet dès le début et garantir la réalisation d'analyses d'impact des risques et l'intégration de technologies respectueuses de la protection des données. Les ressources nécessaires doivent être planifiées dès le départ. En outre, une documentation conforme à la protection des données doit être établie.

L'application Cyclomania de Pro Velo Suisse

Une nouvelle application destinée à encourager l'utilisation du vélo permettra de suivre les utilisateurs enregistrés durant un mois dans l'année. Le Préposé a conseillé Pro Velo Suisse sur les aspects relatifs à la protection des données.

Soutenue par l'Office fédéral de l'énergie, Pro Velo Suisse, organisation faîtière des associations locales et régionales défendant les intérêts des cyclistes en Suisse, a développé la nouvelle application Cyclomania. Cette application est destinée à promouvoir le vélo comme moyen de transport. Les utilisateurs s'inscriront pour participer à cette campagne qui s'étendra sur un mois chaque année et l'application en question créera un profil de leurs déplacements durant ce mois. Les données collectées seront utilisées, d'une part, pour l'établissement de statistiques personnelles des utilisateurs de Cyclomania et le tirage au sort de divers prix. D'autre part, elles seront transmises aux communes participantes sous forme anonymisées et agrégées afin d'aider ces communes à améliorer leurs infrastructures en fonction du comportement de la population. Si les utilisateurs donnent leur consentement, les données pourront être conservées à des fins de recherche au-delà de la durée de la campagne.

Le Préposé a conseillé Pro Velo Suisse sur les aspects du projet liés à la protection des données. Il est notamment important que les utilisateurs soient informés de manière transparente et appropriée de tout traitement de données personnelles et que le principe de proportionnalité soit respecté. Par exemple, les données doivent être effacées dès qu'elles ne sont plus nécessaires aux fins indiquées. En outre, l'utilisateur doit pouvoir le plus facilement possible soit fermer l'application, soit l'utiliser de façon ciblée grâce à des (pré)réglages garantissant la protection des données. Il serait judicieux également que les informations concernant le consentement explicite de l'utilisateur soient courtes et claires, avec des liens directs vers des informations complémentaires. Il convient enfin de souligner qu'il est impossible d'anonymiser les profils de déplacement (cf. ch. 1.1).

1.9 International

Conférence internationale des commissaires à la protection des données à Tirana

La 41e Conférence internationale des commissaires à la protection des données et de la vie privée (CICPDVP) s'est tenue à Tirana, du 21 au 24 octobre 2019 sous l'égide de la Commission de protection des données personnelles albanaise, autour du thème « Convergence and connectivity : raising global data protection standards in the digital age ».

La Conférence a commencé par une séance à huis clos, lors de laquelle les membres se sont entendus sur un cadre qui continue de renforcer la position du groupe en tant que forum international. En effet, elle a marqué le début d'une nouvelle étape de collaboration entre les autorités de protection des données du monde entier. Le nouveau nom choisi pour la Conférence internationale « Global Privacy Assembly – Assemblée globale de la vie privée (GPA) » est le jalon d'une réforme essentielle en terme d'organisation interne, de fonctionnement et de coordination pour l'avenir. Les trois priorités stratégiques de la Conférence sont de : premièrement faire progresser la protection de la vie privée dans le monde à l'ère du numérique ; deuxièmement maximiser la voix et l'influence de la Conférence, notamment en renforçant le rôle de la Conférence dans la politique numérique et les relations avec d'autres organismes et réseaux internationaux ; troisièmement renforcer les capacités pour aider les membres à partager leur expertise tout au long de l'année.

Six documents ont été adoptés lors de la séance à huis clos des 21 et 22 octobre 2019 :

- Résolution sur l'orientation stratégique de la conférence (2019 – 2021)
- Résolution sur la vie privée en tant que droit humain fondamental et condition préalable à la démocratie;
- Résolution sur la promotion d'instruments pratiques nouveaux et à long terme et la poursuite des efforts juridiques en vue d'une coopération efficace en matière de contrôle transfrontalier;
- Résolution sur les médias sociaux et le contenu extrémiste violent en ligne (le PFPDT s'est opposé à ce projet et, à l'instar de représentants d'autres autorités de protection des données, s'est abstenu lors du vote final);
- Résolution visant à soutenir et à faciliter la coopération réglementaire entre les autorités chargées de la protection des données et les autorités chargées de la protection des consommateurs et de la concurrence, afin de mettre en place des normes de protection des données claires et cohérentes dans l'économie numérique;
- Résolution concernant le rôle de l'erreur humaine dans les violations de données à caractère personnel.

M. Edi Rama, Premier Ministre de l'Albanie, a prononcé une allocution lors de la séance ouverte de la Conférence. La caractéristique dominante de cette session ouverte a été l'interaction et la coopération entre les représentants des autorités de protection des données, du monde universitaire, de l'industrie, de la société civile et des médias. Les sujets traités comprenaient des échanges relatifs aux normes communes en matière de protection des données et de la vie privée ; les défis mondiaux en matière de protection de la vie privée des modèles commerciaux basés sur les données ; la protection des données et la concurrence en tant que réglementation numérique convergente ; la responsabilisation en tant que pont global permettant de respecter des normes élevées en matière de protection des données ; et enfin des discussions sur les défis futurs pour les autorités de protection des données et les responsables de la protection des données.

La conférence a rassemblé plus de 700 personnes. Sa prochaine édition aura lieu à Mexico en 2020.

Conférence européenne des commissaires à la protection des données à Tbilissi

Nous avons participé à la Conférence européenne des commissaires à la protection des données focalisée sur les défis de la mise en œuvre du Règlement général sur la protection des données (RGPD) ainsi que sur les nouveautés majeures de la Convention 108+, qui reste le seul instrument international juridiquement contraignant dans le domaine de la protection des données.

La Conférence européenne des commissaires à la protection des données s'est déroulée à Tbilissi (Géorgie) les 8, 9 et 10 mai 2019 à l'invitation de la Commissaire géorgienne à la protection des données. Cette 29e édition a été l'occasion de revenir sur la première année du RGPD : elle a permis aux autorités de protection des données d'assister à des débats sur les défis liés à sa mise en œuvre et à son application. Dans ce cadre, différentes actions effectuées par les autorités de protection des données ont été présentées, notamment un logiciel permettant d'effectuer des analyses d'impact de la Commission nationale informatique et libertés (CNIL), disponible en 16 langues. La portée territoriale et les mécanismes de coopération ont également fait l'objet d'une discussion de panel auquel une représentante du Préposé a participé.

Les participants ont par ailleurs discuté de la Convention 108+ du Conseil de l'Europe qui permettra notamment de faciliter la coopération entre les Parties, de la protection des données des enfants, de la protection des données et des organisations internationales ainsi que du futur de la Conférence. Les principales nouveautés de la Convection 108+ ont été présentées par les experts du panel qui ont tous rappelé que l'entrée en vigueur de ce texte du conseil de l'Europe était d'une importance cruciale pour tous puisque ce texte demeure encore aujourd'hui le seul instrument international juridiquement contraignant dans le domaine de la protection des données.

Association francophone des autorités de protection des données

Une représentante du Préposé a participé à la Conférence annuelle de l'Association francophone des autorités de protection des données (AFAPDP), portée sur le thème du « citoyen numérique » à Dakar. Trouver l'équilibre entre la protection de la sphère privée des individus et les intérêts de toutes les parties prenantes est le défi majeur des autorités de protection des données.

L'Association francophone des autorités de protection des données (AFAPDP) s'est réunie en conférence les 16 et 17 septembre 2019 à Dakar à l'invitation de la Commission de protection des données personnelles du Sénégal et avec le soutien de l'Organisation internationale de la Francophonie. Quatorze délégations étaient représentées à cette occasion. Les présidents, commissaires et représentants des autorités francophones de protection des données personnelles ont accueilli parmi eux le Commissaire à l'information (OIC) de l'île de Jersey, portant ainsi le nombre de membres à 21. La Conférence internationale (CICPDVP) et l'Autorité de régulation des télécommunications (ART) du Cameroun ont été admises comme observateurs. Les membres ont élu un nouveau Bureau.

Enfin, une stratégie d'action à l'horizon 2025 a été adoptée. Celle-ci devrait contribuer à atteindre les trois grands objectifs de l'association, à savoir faire progresser le droit à la protection des données personnelles et à la vie privée dans l'espace francophone, accompagner et renforcer les capacités des membres de l'AFAPDP et faire rayonner l'expertise et la vision francophone au-delà des frontières de la Francophonie.

La Conférence annuelle de l'AFAPDP a porté sur le thème du « citoyen numérique ». Dans l'espace numérique, le sujet de droit est perçu comme un consommateur, un objet d'étude, ou un « troll » anonyme, comme si l'espace numérique était une sphère distincte de la vie réelle, où l'individu devait entrer dans l'une de ces cases. Trouver l'équilibre entre la protection des droits des personnes et la préservation des intérêts des responsables de traitement, sans perdre de vue les progrès et les infinies potentialités que renferme le numérique, représente le défi quotidien auquel les autorités de protection des données sont confrontées. Les données personnelles sont indissociables de la personne humaine. Il est important pour nos autorités de rappeler sans cesse le cœur de leur mission : la protection de la vie privée des personnes.

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

Au cours de la période sous revue, les groupes de coordination chargés de la surveillance se sont réunis à Bruxelles. Ils ont abordé entre autres la question de l'augmentation importante des demandes d'accès au système d'information SIS et adopté deux rapports.

Cette année également, en sa qualité d'autorité nationale de surveillance, le Préposé a participé aux réunions des trois groupes de coordination du contrôle (GCC) des systèmes d'information de l'UE SIS II, VIS (présidence assurée par le Préposé) et Eurodac. Ces réunions ont eu lieu les 19 et 20 juin 2019 et les 26 et 27 novembre 2019 à Bruxelles. 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 SIS II s'est notamment penché sur la question de l'augmentation importante des demandes d'accès au système d'information SIS. Cette augmentation a été observée dans de nombreux États membres, mais surtout en Suisse. Le GCC continuera à traiter ce thème. Le GCC Eurodac a adopté le rapport sur les droits des personnes concernées et le GCC VIS celui sur la formation à la protection des données des personnes autorisées à accéder au VIS.

Ces trois groupes ont également discuté du projet de restructuration les concernant. À l'avenir, les trois GCC seront intégrés en tant que « comité de contrôle coordonné » au Comité européen de la protection des données (European Data Protection Board, EDPB), qui en assurera également le secrétariat. Même si la Suisse n'est pas membre de l'EDPB, elle restera à l'avenir associée aux travaux liés aux domaines Schengen et Dublin.

OCDE : Groupe de travail sur la gouvernance des données et la vie privée dans l'économie numérique

Récemment créé par l'Organisation de coopération et de développement économiques (OCDE), le groupe de travail sur la gouvernance des données et la vie privée dans l'économie numérique (GTGDVP) s'est réuni pour la première fois à Paris en novembre 2019.
Outre la constitution du nouveau groupe de travail, une journée entière a été dédiée, dans le cadre d'une réunion d'experts, aux nouveaux défis à relever dans la mise en œuvre de la protection des données. Le deuxième jour, divers sujets et documents de travail ont été discutés et transmis au Secrétariat pour traitement ultérieur, puis aux membres pour consultation.

La première table ronde a été consacrée aux conséquences de l'intelligence artificielle sur la protection des données personnelles et sur la mise en œuvre des lignes directrices régissant la protection de la sphère privée. Citons ici quelques-unes des questions traitées : Quels sont les défis que doivent relever les autorités de protection des données dans le contexte de l'intelligence artificielle (IA), à l'occasion de la mise en œuvre des principes fondamentaux des directives de protection des données et des audits ? Dans quelle mesure les lignes directrices actuelles de la politique en matière d'IA tiennent-elles compte de la sphère privée et de la protection des données ? Comment garantir l'exercice des droits individuels ?

La deuxième table ronde a porté sur l'augmentation des flux transfrontaliers de données personnelles et sur l'importance croissante de la coopération internationale visant à mettre en œuvre le respect de la sphère privée et la protection des données. Différentes possibilités de coopération ont été identifiées et les questions suivantes ont été abordées : comment la coopération internationale peut-elle contribuer à la fiabilité du flux transfrontalier de données personnelles ? Quels sont les obstacles à la coopération internationale et comment les lever ? Quels enseignements tirer de la coopération ?

La troisième table ronde a permis de faire le point sur les discussions de la journée et d'examiner comment l'OCDE peut répondre pour le mieux aux défis en la matière.

Lors de la session restreinte, les premières ébauches de rapports intérimaires, d'enquêtes et de documents de travail ont été discutées. Elles portaient sur les thèmes suivants : amélioration de l'accès aux données et leur partage, portabilité des données, éthique des données, guide pratique pour la mise en œuvre de l'intelligence artificielle et promotion de la comparabilité dans le signalement des atteintes à la protection des données. Le groupe de travail s'est également penché sur la Recommandation de 2012 concernant la protection des enfants sur Internet, actuellement en cours de révision. Enfin, le Secrétariat a présenté un premier rapport intermédiaire faisant le point sur la mise en œuvre des lignes directrices sur la protection des données.

Réunions plénières du Comité européen de la protection des données

En 2019, le Préposé a participé à deux réunions plénières du Comité européen de la protection des données (CEPD/ European Data Protection Board, EDPB) sur des questions liées à Schengen et à la dernière réunion plénière de 2019 pour un échange général d'informations.

Le CEPD, institué par le RGPD, a tenu douze réunions plénières en 2019. Notre participation en tant qu'observateurs aux sessions plénières a été limitée aux sujets liés à Schengen.

Ainsi, pour la première fois depuis la création de le CEPD, nous avons participé à deux réunions plénières et, avec d'autres autorités de protection des données, avons pu exprimer notre position sur les compétences nationales. En outre, au début du mois de décembre 2019 et à l'invitation du Comité, le Préposé a fourni à celui-ci de brèves informations sur l'état de sa procédure ouverte contre l'association Libra, basée à Genève (cf. Accent II, Projet Libra).

Groupe de travail européen de traitement de cas pratiques en matière de protection des données

Un représentant du Préposé a participé à la 31e édition de l'Atelier européen de cas pratiques « Case Handling Workshops ».

Le nouveau Contrôleur européen à la protection des données, Wojciech Wiewiórowski, a accueilli les 28 et 29 novembre 2019 la 31e édition annuelle de l'Atelier européen de traitement de cas pratiques à Bruxelles. Ont participé à cet atelier des collaborateurs de 28 autorités chargées de la protection des données de pays membres de l'UE et de pays tiers, dont un représentant du Préposé.

Cet atelier a permis de partager les expériences relatives à l'examen des plaintes, des conseils aux responsables du traitement et de l'application des lois sur la protection des données. Au cours de ces deux jours, des cas d'application portant sur six thèmes principaux ont été étudiés : recours à des prestataires informatiques de la part des institutions publiques ; traitement des demandes manifestement infondées ou excessives au titre de l'article 57, paragraphe 4, RGPD ; traitement des cas au titre de l'article 56, paragraphe 2, RGPD (compétence locale additionnelle s'ajoutant à celle de l'autorité principale) ; évaluation des demandes de consultation préalable au titre de l'article 36, paragraphe 3, RGPD ; systèmes d'information sur le crédit et intermédiaires de données ; exercice des pouvoirs d'enquête et de correction et mise en balance des différentes options au titre de l'article 58, RGPD.

Sous-groupe de travail « Border, Travel & Law Enforcement »

Nous avons participé aux sept réunions du sous-groupe de travail « Border, Travel & Law Enforcement subgroup » (BTLE) au cours de l'année sous revue. Le sous-groupe a suivi avec attention le troisième examen du bouclier de protection de données entre l'UE et les États-Unis et continue à accompagner « l'accord parapluie » (« Umbrella Agreement ») qui encadre les échanges de données personnelles en matière de police et de justice pour la communication des données PNR.

Le « Border, Travel & Law Enforcement » (BTLE) est un sous-groupe de travail créé par l'ancien Groupe de travail « Article 29 » sur la protection des données. Le sous-groupe a pour mission de suivre les développements législatifs touchant aux secteurs de la police, des frontières et de la justice pénale, notamment ceux relevant de l'acquis Schengen. Dans ce contexte, il prépare des avis et des positions qui sont ensuite adoptés par le Comité européen.

Le sous-groupe s'est en particulier concentré sur l'avenir des modèles de surveillance des grands systèmes informatiques de l'UE dans le domaine de la justice et de la politique intérieure. Il s'est penché sur l'élaboration de nouvelles règles de procédure.

Il a accompagné avec attention particulière le troisième examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis. Le groupe a suivi avec attention les travaux concernant le protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et a préparé une position commune pour la Conférence Octopus.

Il a continué à accompagner «l'accord parapluie» (« Umbrella Agreement ») qui encadre les échanges de données personnelles en matière de police et de justice, en limitant les droits des administrations américaines dans le traitement des données européennes et la création d'un cadre européen pour la communication des données PNR aux pays tiers et pour l'utilisation des données PNR à des fins répressives.

Règlement européen sur la protection des données

Le nouveau Règlement européen sur la protection des données (RGPD) est également applicable aux traitements de données par les entreprises suisses à certaines conditions. En participant à différentes conférences internationales, le Préposé a assisté aux débats sur les défis liés à l'application du nouveau règlement européen. Plus d'un an après son entrée en vigueur, de nombreuses questions restent ouvertes, notamment sur le champ d'application territorial.

Adopté le 27 avril 2016, le Règlement européen sur la protection des données personnelles (RGPD) est applicable directement dans tous les Etats membres de l'Union européenne depuis le 25 mai 2018. Son champ d'application est toutefois bien plus vaste que le seul territoire de l'Union européenne : en effet, dès lors qu'il propose des biens ou des services à des personnes se trouvant au sein de l'Union européenne, ou qu'il observe le comportement desdites personnes notamment pour analyser leurs préférences, le responsable de traitement (ou le sous-traitant) est soumis aux exigences du RGPD, même s'il n'est pas établi dans l'Union. Tout au long de l'année sous revue, le Préposé a participé à différentes conférences internationales qui lui ont permis d'assister à des débats sur les réalisations et les défis liés à la mise en œuvre et à l'application de ce texte de référence. La portée extraterritoriale du règlement et les mécanismes de coopération ont aussi été évoqués. Les autorités francophones européennes non membres de l'Union européenne étant confrontées aux mêmes difficultés, elles ont échangé tout au long de l'année afin de discuter sur l'entrée en vigueur du RGPD, de partager leurs expériences et mettre en commun les questions qui leur ont été adressées afin de coordonner leurs réponses.

Le Préposé a poursuivi sa participation à des nombreuses séances d'information à ce sujet tant auprès de l'administration fédérale qu'auprès de privés. Dans le cadre de son activité de conseil, il a également répondu à de nombreuses questions orales et écrites des citoyens et des médias.

Plus d'un an après l'entrée en vigueur du RGPD, le Comité Européen de la Protection des Données (European Data Protection Board, EDPB), l'organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne, a enfin publié ses lignes directrices sur le champ d'application du RGPD après avoir fait l'objet d'une consultation publique à laquelle le Préposé a participé en collaboration avec l'autorité monégasque de protection des données (CCIN-Commission de contrôle des informations nominatives) afin de demander la clarification d'un certain nombre d'éléments sur cette question hautement importante pour les pays tiers intégrés au paysage de l'Union. Une réunion a par ailleurs eu lieu à Berne en février 2020 afin d'analyser cette nouvelle version. Les informations relatives à l'application du RGPD sont régulièrement mises à jour sur notre site internet.

Le Brexit et la transmission de données personnelles

À la suite du référendum britannique de juin 2016 sur le retrait de l'Union européenne (Brexit), le gouvernement britannique a notifié sa décision à l'UE. Le retrait a eu lieu le 1er février 2020 au terme de plusieurs reports.
Comme déjà mentionné dans le précédent rapport d'activités, le Préposé a participé à de nombreuses réunions avec les autorités de la Confédération et les autorités compétentes du Royaume-Uni afin de garantir que la libre circulation des données personnelles entre la Suisse et le Royaume-Uni reste possible même après le Brexit. Le Royaume-Uni est considéré comme un pays disposant d'un niveau de protection adéquat et le Préposé ne voit actuellement aucune raison de modifier son statut.

L'UE décidera d'ici la fin de l'année 2020 si elle reconnaît l'adéquation de la législation sur la protection des données du Royaume-Uni. Le Préposé suit avec attention l'évolution de la situation.

Le Comité consultatif de la Convention 108

Le Comité consultatif de la Convention 108 (T-PD) a adopté des lignes directrices sur l'intelligence artificielle et la protection des données.
Ces lignes directrices visent à aider les décideurs politiques, les développeurs de l'intelligence artificielle (IA), les fabricants et les prestataires de services à garantir que les applications d'IA ne portent pas atteinte au droit à la protection des données. Elles font référence à d'importants enjeux déjà abordés dans les lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées.

Le T-PD a également adopté un avis sur le projet de Recommandation du Comité des Ministres aux États membres concernant « les conséquences des systèmes algorithmiques pour les droits de l'homme », soumis pour commentaires par le Comité directeur sur les médias et la société de l'information. Il a décidé du programme de travail du comité pour 2020–2021 qui comprendra notamment le suivi de la modernisation de la Convention, la promotion de la Convention, une recommandation spécifique concernant la reconnaissance faciale, le traitement des données personnelles dans le contexte des systèmes éducatifs et un réexamen du profilage. Il travaille en outre sur les mécanismes de suivi et d'évaluation de la Convention 108+ et a décidé de mettre en place un groupe de travail composé des membres du Bureau et de toute délégation intéressée, qui sera chargé de poursuivre l'élaboration des propositions du nouveau mécanisme.

Décision d'adéquation du niveau suisse de protection des données

La Commission européenne a poursuivi son processus d'évaluation de la décision d'adéquation de la Suisse qui date de 2000. Elle devrait rendre ses conclusions en mai 2020. Le maintien de cette décision est l'une des priorités du Conseil fédéral.
Une décision d'adéquation est une décision prise par la Commission européenne et établissant qu'un pays tiers, par l'intermédiaire de sa législation interne ou de ses engagements internationaux, offre un niveau de protection des données personnelles comparable à celui garanti dans l'Union européenne. Grâce à une telle décision, les données personnelles peuvent circuler en toute sécurité entre l'Espace économique européen (EEE) et le pays tiers concerné, sans que des garanties spécifiques ne doivent être mises en place par les responsables du traitement eux-mêmes.

En vertu de l'article 45, al. 3 et 4 du RGPD, la Commission européenne suit l'évolution du niveau de protection des données des pays tiers qui, comme la Suisse, bénéficient d'une décision constatant le caractère adéquat du niveau de protection. Tous les Etats tiers au bénéfice d'une décision d'adéquation sont évalués selon la même méthodologie.

La Commission doit notamment prendre en considération l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes et les engagements internationaux pris par le pays tiers.

La signature de la Convention 108+ en novembre 2019 tout comme la révision de la LPD joueront un rôle important pour le maintien de la décision. Le maintien de cette dernière est d'ailleurs l'une des priorités du Conseil fédéral (cf. Interpellation 17.4088).

Le processus d'évaluation a officiellement commencé en mars 2019 et se poursuit avec des échanges réguliers jusqu'au printemps 2020. Tout au long de l'année sous revue, le Préposé a participé au groupe de travail dirigé par l'Office fédéral de la justice (OFJ). La Commission européenne a jusqu'au 25 mai 2020 pour rendre les conclusions de son évaluation et renouveler la décision concernant la Suisse. En vertu du RGPD, les décisions d'adéquation restent valables jusqu'à ce qu'elles soient modifiées, remplacées ou annulées.

Projet Libra

Le projet de cryptomonnaie Libra a suscité un très vif intérêt dans les médias et auprès des professionnels de la protection des données dans le monde entier. Au cours d'une procédure préliminaire, le Préposé a confirmé sa compétence en tant qu'autorité de surveillance des traitements de données effectués par l'association Libra, basée à Genève, et a requis la remise d'une documentation appropriée. L'association Libra a assuré au Préposé qu'elle mettrait en œuvre les mesures nécessaires à la protection de la sphère privée.

C'est par la presse que le Préposé a appris l'existence de Libra, projet de cryptomonnaie initié par Facebook au niveau mondial. Il a donc été informé par ce biais des déclarations de David Marcus, vice-président pour les produits de messagerie de Facebook, lors de l'audition du 16 juillet 2019 devant une commission du Sénat américain sur le projet de cryptomonnaie de l'association Libra, ainsi que sur la fonction de gouvernance de l'association Libra et le rôle d'autorité de surveillance du Préposé.

Le Préposé n'ayant pas été informé au préalable par les promoteurs de ce projet, il a contacté l'association Libra à Genève par lettre du 17 juillet 2019. Dans cette lettre, il déclarait prendre acte des déclarations de David Marcus selon lesquelles la protection des données serait prise en compte comme élément fondamental du projet. En parallèle, le Préposé précisait qu'il partait du principe qu'en cas de traitement de données personnelles, une analyse d'impact des risques sur la protection des données serait élaborée, qui décrirait entre autres les procédures de traitement prévues, évaluerait les risques en matière de protection des données pour les personnes concernées et énumérerait les mesures appropriées pour réduire ces risques. De plus, il demandait à l'association Libra de lui soumettre la documentation nécessaire sur l'état actuel du projet.

L'association ayant remis en temps voulu les informations requises sur le projet Libra demandées par le Préposé, une rencontre a eu lieu à Berne le 17 septembre 2019 entre ce dernier et les représentants de l'association Libra. Celle-ci a réitéré son engagement à développer un standard de protection des données uniforme au niveau mondial qui répondrait notamment aux exigences du Règlement général de l'UE sur la protection des données. Ce point correspond aux attentes du Préposé, qui entend assurer un haut niveau de protection des données personnelles des utilisateurs. En outre, l'association a affirmé vouloir associer rapidement le Préposé à ses travaux de développement en cours afin de respecter d'emblée les exigences de la législation sur la protection des données, conformément au principe de privacy by design. L'association Libra a assuré par écrit au Préposé qu'elle prendra à temps, c'est-à-dire avant le lancement de la cryptomonnaie, les mesures nécessaires à la mise en place du standard uniforme de protection des données, comme la création d'un service responsable de la protection des données, et chargera ce dernier de procéder à une analyse d'impact des risques. Dans sa lettre datée du 17 février 2020, l'association Libra a informé le Préposé que les travaux sur cette question étaient toujours en cours. Elle a également réaffirmé sa volonté de mettre en œuvre les mesures promises au Préposé afin de protéger les droits de la personnalité dans le cadre du projet Libra.

Depuis qu'il est informé de sa compétence dans la surveillance du projet Libra, le Préposé est en contact avec ses collègues des autorités européennes de protection des données et transmet régulièrement au Comité européen de la protection des données les informations dont il dispose sur l'avancement des travaux. Le 23 août 2019, une rencontre a également eu lieu avec la Commission des services financiers de la Chambre des représentants américaine, présidée par le Secrétariat d'État aux questions financières internationales (SFI), au cours de laquelle le Préposé a fourni des informations sur l'état de sa procédure de contrôle (cf. infra). Le Préposé est également en contact avec la Banque nationale suisse et avec la FINMA afin de coordonner les activités des organes fédéraux et d'assurer un échange d'informations. La FINMA s'est engagée à le tenir informé de l'état de la procédure en cours pour l'octroi d'une licence bancaire, ce qui permet au Préposé de synchroniser sa propre procédure.

Comme il l'a fait jusqu'ici, le Préposé fédéral continuera à informer le public en lui communiquant les mises à jour sur les développements pertinents de son contrôle.

Rencontres et activités internationales

Le 23 août 2019, le Préposé a participé avec d'autres autorités fédérales à une réunion organisée à Berne par le Secrétariat d'État aux questions financières internationales (SFI) où six membres de la Commission des services financiers de la Chambre des représentants des États-Unis, dirigée par sa présidente Maxine Waters, ont été reçus. Ils désiraient se renseigner sur la surveillance administrative des activités de l'association Libra, basée à Genève, et sur le cadre juridique des cryptomonnaies en Suisse, ainsi que sur les implications possibles pour les droits de la personnalité des particuliers concernés aux États-Unis. Le Préposé a informé sommairement la délégation sur la procédure en cours contre l'association Libra et répondu à leurs questions.

Le Préposé a expliqué qu'il était, à l'instar des autres autorités de protection des données, concerné par le projet Libra et son réseau mondial et qu'il se souciait de soutenir la communauté internationale des autorités de protection des données dans leurs efforts conjoints pour protéger la population. Il a ajouté qu'il restait en contact étroit avec le Comité européen de protection des données (CEPD) et la Global Privacy Association (actuellement GPA, anc. ICDPPC) ainsi qu'avec d'autres autorités de protection des données. Il a confirmé plus particulièrement que la procédure suisse ne porterait en rien préjudice aux compétences et pouvoirs des autres autorités de protection des données d'autres pays ni ne les influencerait. Il a précisé en outre qu'il préviendrait les éventuelles tentatives de monter les autorités de protection des données les unes contre les autres. Enfin il a informé les présidents de le CEPD et de la GPA qu'il les tiendrait brièvement informés de la procédure en Suisse.

Le 16 septembre 2019, un représentant du Préposé a également participé à un groupe de discussion sur la protection des données dans le cadre d'une conférence organisée à Bâle par la Banque des règlements internationaux sur les cryptomonnaies dites « stables ». Les participants étaient pour l'essentiel des représentants de banques nationales et d'autorités de régulation financière. C'était la première fois que des thèmes relatifs à la protection des données pouvaient être mis en lumière et discutés dans un tel cadre.

Le Préposé a été en contact à plusieurs reprises avec des représentants de la GPA et de le CEPD. À l'occasion de la Conférence internationale des commissaires à la protection des données et à la vie privée qui s'est tenue à Tirana, le Préposé a eu l'occasion de rencontrer personnellement les commissaires à la protection des données de différents États européens et de la Commission fédérale du commerce américaine (Federal Trade Commission, FTC). Le Préposé a également été en contact avec des représentants de la Banque nationale suisse et de l'Autorité fédérale de surveillance des marchés financiers (FINMA), qui le tiendront informé du calendrier des procédures d'autorisation conformément au droit des marchés financiers concernant l'Association Libra.

En outre, le 3 décembre 2019, le Préposé a participé à une réunion de le CEPD à Bruxelles pour un échange d'informations (cf. ch. 1.9).

Principe de la transparence

2.1 Généralités

Depuis l'introduction de la loi sur la transparence, force est de constater que le changement de paradigme continue sa progression et que le principe de la transparence est appliqué, avec succès, par la plupart des autorités fédérales. Ce constat est vérifié par les chiffres présentés ci-après qui confirment la tendance des années passées, à savoir une prédominance de l'accès complet aux documents demandés et une augmentation marquée du nombre de demandes d'accès (cf. ch. 2.2).

Plus que jamais, l'année 2019 a montré l'efficacité des médiations orales. Pas moins de 61 % des cas ont été résolus par une solution amiable. Cette manière de procéder doit continuer à être encouragée et favorisée. Plusieurs accords ont non seulement permis au demandeur d'obtenir rapidement des informations, mais également d'avoir un contact direct avec l'administration, voire de nouer des liens étroits pour de futures collaborations avec les autorités fédérales.

Selon la configuration des différentes affaires, il demeure difficile de mener à bien une procédure de médiation dans le délai légal de 30 jours. C'est notamment le cas dans les procédures complexes à trois ou plusieurs parties, concernant des demandes d'accès à des documents qui contiennent des informations en rapport avec le secret d'affaires ou la protection de la sphère privée des particuliers ou d'agents de l'administration. Ces procédures de médiation nécessitent de vastes clarifications, parfois complexes, avec les parties concernées, ce qui se traduit inévitablement par un allongement de la durée de la procédure (cf. ch. 2.3).

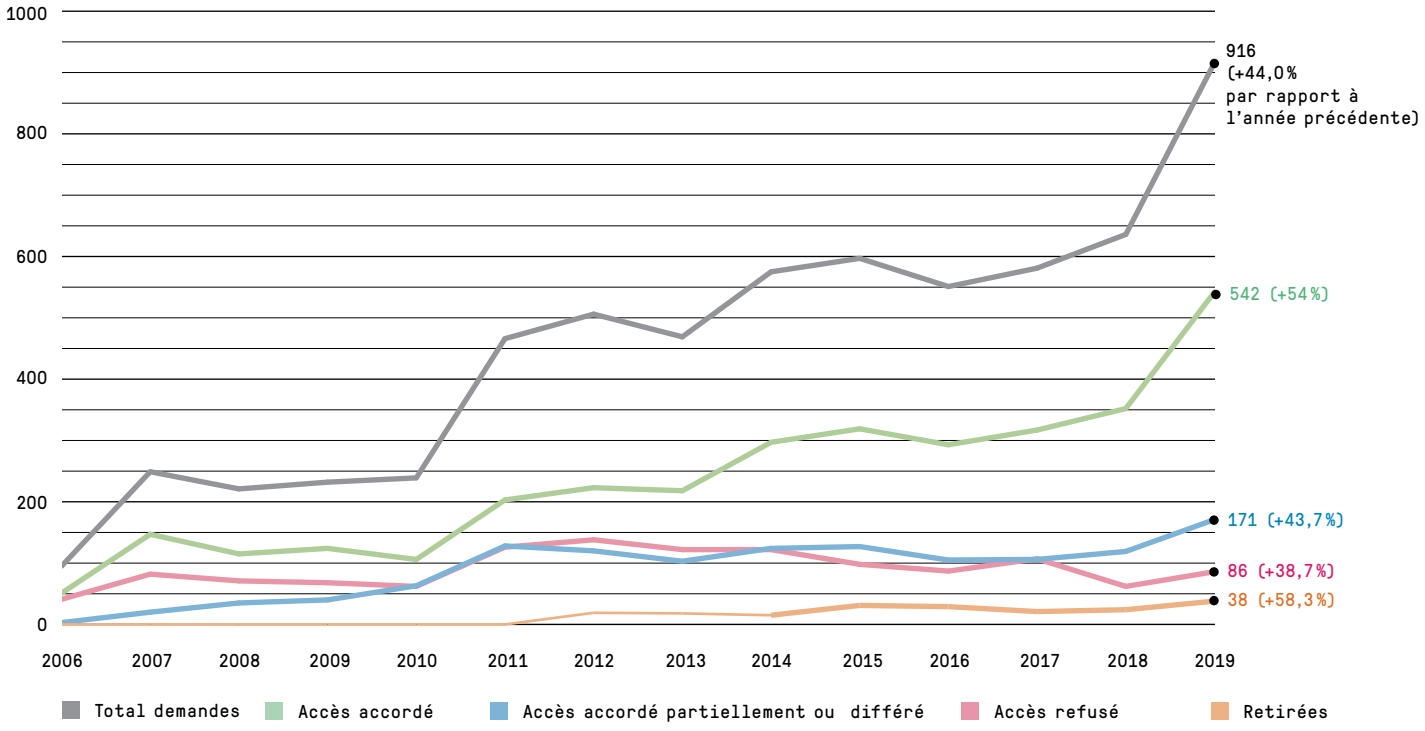
Cette année encore, la loi sur la transparence a prouvé qu'elle était un outil précieux de promotion de la transparence, d'information, de contrôle à destination de la population et que, de ce fait, il convient de rester vigilant et d'éviter qu'elle ne soit détournée de son but par l'introduction de nouvelles dispositions légales visant à exclure son application. Au cours de l'année sous revue, certains secteurs de l'administration (dont l'Administration fédérale des douanes et l'Office fédéral de la santé publique) ont à nouveau déployé des efforts accrus pour exclure de la transparence une partie de leurs activités ou certaines catégories de documents (cf. ch. 2.4). En revanche, le législateur a montré son attachement au principe de la transparence au travers de la loi fédérale de juin 2019 sur les marchés publics (LMP), ainsi que par la décision de la Commission des institutions politiques du Conseil national sur le principe de gratuité des demandes d'accès. Malheureusement, dans ses dispositions d'exécution de la LMP, le Conseil fédéral a de nouveau partiellement limité la transparence qui avait été introduite contre son gré dans cette loi (cf. ch. 2.4).

2.2 Demandes d'accès – nouvelle hausse en 2019

Selon les chiffres communiqués par les autorités fédérales, 905 demandes d'accès leur ont été soumises en 2019 (contre 636 en 2018). Cette augmentation s'explique en partie par le fait que l'OFSPO à lui seul a comptabilisé 175 demandes d'accès. En incluant le Ministère public de la Confédération (10) et les Services parlementaires (1), le total se monte à 916 (soit 44 % de plus qu'en 2018). Le fait que la population, en particulier grâce à la bonne couverture médiatique, soit de mieux en mieux informée au fil des années sur le principe de la transparence et qu'elle utilise maintenant elle-même de manière plus active les possibilités qu'offre ce principe, a probablement aussi contribué à l'augmentation des chiffres.

Il est probable que cette tendance se poursuivra dans les années à venir, d'autant plus que l'on observe une augmentation générale des attentes émanant des citoyens en matière de transparence, s'agissant de l'administration et du monde politique. Dans 542 cas (59 %), les autorités ont accordé un accès complet (contre 352 en 2018, soit 55 %). Par ailleurs dans 171 cas (19 %), les demandeurs ont reçu un accès partiel aux documents et dans 86 cas (9 %), l'accès leur a été entièrement refusé (contre 62 en 2018, soit 10 %). Les autorités ont précisé que 38 demandes d'accès avaient été retirées (contre 24 en 2018, soit 4 %), que 43 demandes étaient encore en suspens fin 2019 et que dans 36 cas, aucun document officiel n'existait. Depuis 2015, dans plus de 50 % des cas, un accès complet est accordé aux documents demandés. En comparaison, le nombre des demandes d'accès entièrement refusées reste minoritaire et se stabilise au fil des ans aux alentours de 10 %. Le Préposé note que la pratique des autorités tend vers plus de transparence. Les mesures prises dans ce sens par plusieurs autorités fédérales ont contribué à l'augmentation du nombre d'accès accordés et renforcent le changement de paradigme souhaité par le législateur (cf. égal. les statistiques détaillées figurant au ch. 3.3).

Graphique 1 : Demandes d'accès – évolution depuis 2006



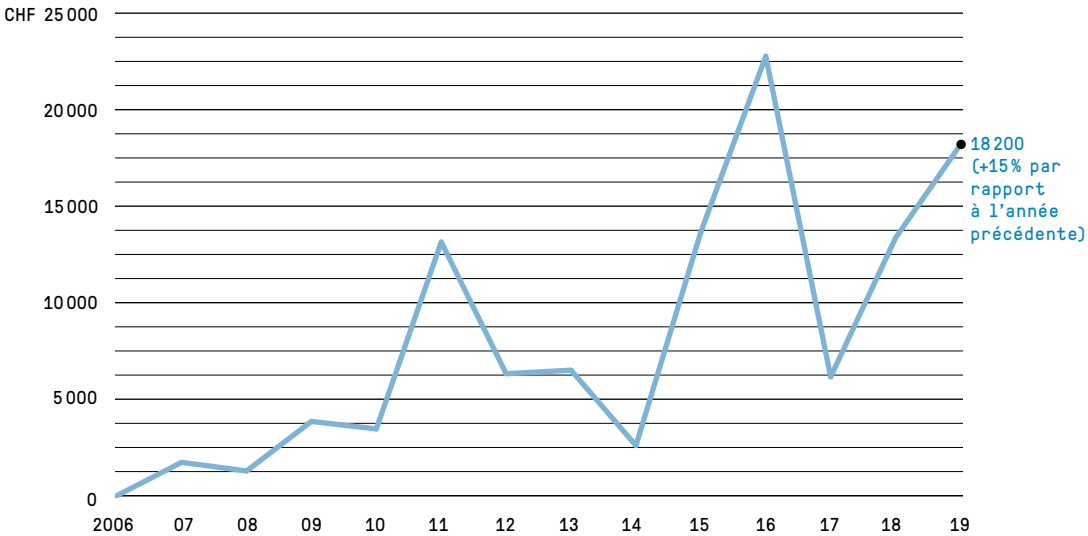
Départements et offices fédéraux

Au niveau des offices, il ressort des chiffres communiqués que l'OFSPO a reçu le plus de demandes d'accès en 2019 (175), suivi par l'OFEV et l'OFSP avec chacun 35 demandes puis par le SECO (34). Les départements ayant reçu le plus de demandes sont le DDPS (225) ainsi que le DFAE (168). Dix autorités ont en revanche annoncé qu'aucune demande d'accès ne leur avait été soumise durant l'année sous revue. Le Préposé s'est pour sa part vu adresser dix demandes; dans six cas l'accès a été entièrement accordé, dans un cas le document demandé n'existait pas et dans trois cas, les demandes ont été retirées.

En 2019, le montant total des émoluments prélevés pour obtenir l'accès à des documents officiels s'élève à 18185 francs. Il s'agit donc d'un montant plus élevé qu'en 2018 (13358 francs), mais qui reste dans la norme au regard des années précédentes. Le DFJP et la Chancellerie fédérale n'ont prélevé aucun émolument, les six autres départements ont partiellement facturé leur temps de travail aux demandeurs (DFI : 8710 francs ; DDPS : 300 francs ; DFF : 3750 francs ; DEFR : 700 francs ; DETEC : 2750 francs). Il convient de relever que seul 31 des 916 demandes d'accès ont entraîné le prélèvement d'un émolument. Ce chiffre est certes plus important qu'en 2018 où seules 17 demandes en avaient fait l'objet, mais le nombre de demandes d'accès est bien plus élevé. Comme lors des années passées, la perception d'un émolument constitue l'exception ; la gratuité étant accordée dans près de 97 % des cas. Le Préposé remarque néanmoins qu'au cours de l'année sous revue, les autorités fédérales ont désormais tendance à prélever de plus petites sommes, mais plus régulièrement.

Dans le cadre de la mise en œuvre de l'initiative Graf Litscher (16.432 n Iv. pa. Graf-Litscher. Principe de la transparence dans l'administration. Faire prévaloir la gratuité de l'accès aux documents officiels), la Commission des institutions politiques du Conseil national a constaté que certains départements avaient déjà facturé des prestations de plusieurs milliers de francs, contribuant à vider de sa substance le principe de l'accès aux documents officiels. Elle estime donc qu'il est juste d'inscrire dans la loi le principe de la gratuité et à cet effet, a mis en consultation le 14 février 2020 un projet de révision de la loi sur la transparence allant dans ce sens.

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



Au sujet des heures de travail consacrées au traitement des demandes d'accès, le Préposé souligne à nouveau que les autorités ne sont pas tenues de les enregistrer et qu'il n'existe aucune directive de saisie uniforme pour l'ensemble de l'administration fédérale. Les indications qui lui sont transmises le sont sur une base volontaire et ne reflètent que partiellement les heures de travail effectives pour le traitement des demandes. Selon ces données, le temps de travail annoncé pour l'année sous revue, soit 4375 heures, a diminué par rapport à 2018 (4827 heures). Cette diminution se constate également au niveau des heures de travail investies dans la préparation des séances de médiation qui totalisent 473 heures (contre 672 heures en 2018 et 914 heures en 2017). Ce faible nombre d'heures n'est pas en adéquation avec la nette augmentation du nombre de procédure de médiation. Il paraît vraisemblable que l'ensemble des heures investies à la préparation des procédures n'ait pas été entièrement comptabilisé. De plus, dans bien des cas, le temps consacré à la rédaction des décisions ou aux procédures de recours n'a pas été communiqué au Préposé.

Services parlementaires

Les Services parlementaires nous ont annoncé avoir reçu une seule demande à laquelle ils ont répondu par un refus d'accès entier.

Ministère public de la Confédération

Le Ministère public de la Confédération nous a communiqué avoir reçu dix demandes en 2019. L'accès a été accordé dans trois cas et entièrement refusé dans un cas. Parmi les demandes restantes, il n'existait pas de document pour deux d'entre elles, trois autres ont été retirées et la dernière est en suspens.

2.3 Procédures de médiation – Augmentation considérable des demandes en médiation

En 2019, 133 demandes en médiation ont été déposées auprès du Préposé contre 76 en 2018, ce qui représente une augmentation de 75 %. Les médias (34), les privés (40) et les entreprises (47) sont à l'origine de la majorité des demandes. Ces chiffres permettent le constat suivant ; parmi les 258 cas pour lesquels l'administration fédérale a refusé entièrement ou partiellement l'accès, 132 ont fait l'objet d'une demande en médiation auprès du Préposé, soit 51 % de l'ensemble des demandes d'accès non satisfaites.

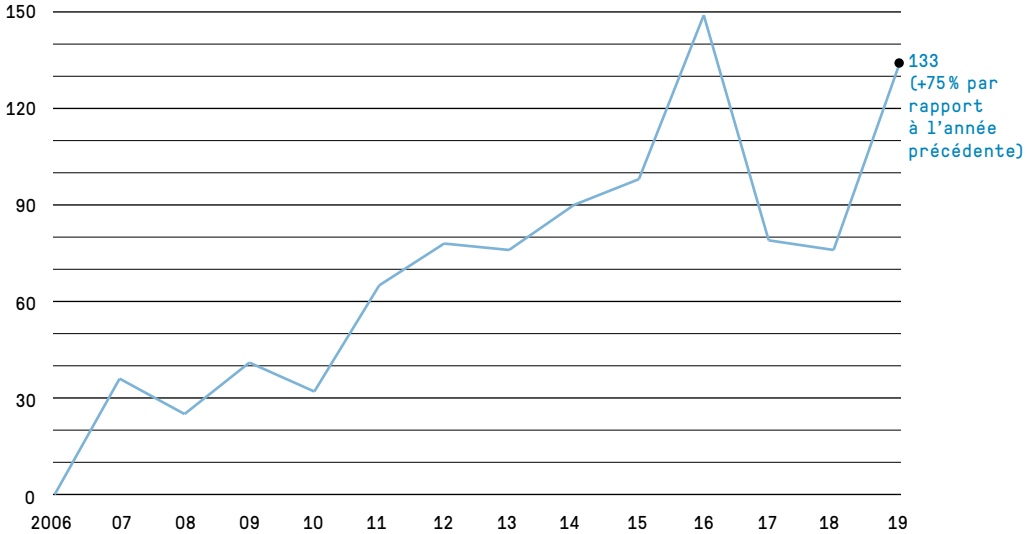
Cette augmentation du nombre de demandes en médiation s'explique en partie par le fait qu'une demande d'accès a entraîné la consultation de très nombreux tiers concernés et que 28 d'entre eux ont déposé, suite à la consultation, des demandes en médiation auprès du Préposé.

Il sied de relever que cet accroissement du nombre de demandes génère une masse de travail importante et a eu un impact évident sur la charge de travail du Préposé. 108 demandes en médiation ont été réglées en 2019 dont 93 avaient été soumises au cours de cette même année et 15 en 2018.

Dans la majorité des cas (48), une solution consensuelle a été trouvée entre les participants.

Le Préposé a également émis 26 recommandations ayant permis de clore 31 cas dans lesquels une entente entre les parties n'était pas envisageable. Parmi les cas réglés, il faut aussi tenir compte des six demandes en médiation qui ont été retirées sans que le Préposé n'ait dû intervenir, des huit cas où les conditions d'application de la loi sur la transparence n'étaient pas remplies ainsi que des douze demandes qui n'avaient pas été soumises dans les délais. À la fin de l'année, quatre procédures de médiation étaient suspendues conformément à la volonté des participants.

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



Durée du traitement

Le tableau ci-dessous est divisé en trois parties en fonction des durées de traitement. Il met en évidence qu'en 2019 la majorité des procédures ont été résolues dans le délai d'ordre de 30 jours. Il sied de préciser que la durée de traitement ne prend pas en compte la durée durant laquelle une procédure de médiation est suspendue avec l'accord des participants. Une suspension de la procédure de médiation intervient en particulier lorsqu'après la séance de médiation, une autorité souhaite réexaminer sa position ou qu'elle doit procéder à la consultation de tiers concernés.

Les dépassements du délai sont souvent la conséquence de l'absence des personnes ou des autorités concernées (vacances, maladies, déplacements), d'un grand nombre de tiers concernés par la procédure ou du traitement de questions juridiques complexes. Ces explications sont également valables pour les quatre cas (dont trois procédures où les causes ont été jointes) qui ont dépassé les 100 jours de traitements.

A cela s'ajoute le fait qu'en raison de consultations à l'étranger, de multiples tentatives de négociation entre les participants et du nombre de document ou personnes concernées, les délais ne pouvaient pas être respectés. A noter que les situations susmentionnées engendrent fréquemment un surcroît important de travail et dans ces cas, le Préposé peut, conformément à l'article 12a de l'ordonnance sur le principe de la transparence dans l'administration (OTrans; RS 152.31), prolonger d'une durée raisonnable le délai d'ordre.

La comparaison avec les années précédentes permet de constater que depuis la mise en œuvre de l'essai pilote en 2017, la durée de traitement des procédures de médiation a fortement diminué. Les chiffres de l'année 2019 confirment clairement cette réduction notable et une fois mis en corrélation avec la proportion de solutions amiables, ils démontrent l'efficacité des mesures prises, notamment de l'accent mis sur la médiation orale.

En général, le délai légal de 30 jours pour mener une procédure de médiation peut être respecté lorsque les séances de médiation se déroulent comme prévues, c'est-à-dire sans demande de report par les parties concernées, et qu'elles se concluent avec succès par un accord dans le délai suivant la réception de la demande. Si aucun accord n'est conclu, la recommandation écrite ne peut pas systématiquement être remise aux parties dans les 30 jours suivant la réception de la demande. Par contre, lorsque de nombreuses demandes en médiation sont déposées sur une courte période, il n'est d'emblée pas possible de respecter le délai pour de raisons évidentes de ressources. S'il y a déjà des retards dans le traitement des procédures de médiation, chaque nouvelle demande contribue à accentuer ces retards. Dans les affaires complexes et dans les procédures multipartites (c'est-à-dire impliquant plusieurs tiers concernés), les 30 jours s'avèrent également (trop) courts. L'expérience montre en outre que lorsque des tiers consultés font appel à un avocat dès la procédure d'accès et de médiation, cela est peu propice à une solution simple, rapide et pragmatique.

Tableau 1 : Durée de traitement des procédures de médiation

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

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

Proportion des solutions amiables

L'efficacité des mesures instaurées en 2017 et des séances de médiation s'évalue surtout par la proportion de solutions amiables au regard des recommandations. Les solutions amiables présentent de nombreux avantages, elles permettent entre autres d'éclaircir les faits, d'accélérer la procédure d'accès aux documents ou de créer les bases d'une éventuelle collaboration future entre les participants à la séance de médiation. Au cours de l'année sous revue, 48 solutions amiables ont été trouvées et 26 recommandations ont été émises par le Préposé pour résoudre 31 cas, ce qui correspond à 61 % de solutions amiables par rapport aux recommandations. Le Préposé relève que la proportion des procédures de médiation qui se sont conclues par une solution amiable a encore augmenté.

À titre d'information, toutes les recommandations émises pendant l'année sous revue sont disponibles sur le site internet du Préposé (www.leprepose.ch).

Tableau 2 : Solutions amiables

2013 – 2016	40 %
2017	60 %
2018	55 %
2019	61 %

Nombre des cas pendants

Les chiffres indiqués ci-dessous renseignent sur le nombre de cas pendants à la fin des années sous revue. Début janvier 2020, le nombre de cas encore pendants de l'année 2019 se montait à 43, dont quatre procédures suspendues.

Il convient de préciser que 42 demandes en médiation ont été déposées dans le courant des mois de novembre et décembre 2019 et que 40 d'entre elles ont été réglées avant la mise sous presse. Toutefois, ce nombre de cas pendants, bien plus haut que les années précédentes, est la conséquence logique de la forte augmentation du nombre de demandes en médiation et des ressources limitées dont dispose le Préposé. Faute de moyen complémentaire, le risque est grand que les durées de traitement s'allongent, que le délai d'ordre ne puisse plus être respecté et que le nombre de cas pendants en fin d'année prochaine s'accroisse encore.

Tableau 3 : Procédures de médiation pendantes

Fin 2016	33
Fin 2017	3 (2 en traitement; 1 en suspens)
Fin 2018	15 (dont 13 terminées et 2 en suspens en février 2019)
Fin 2019	43 (dont 40 terminées avant la clôture de la rédaction et 3 en suspens)

2.4 Consultation des offices

Consultation des offices relative au projet de loi sur la douane et la sécurité des frontières, ouverture de la procédure de consultation

L'Administration fédérale des douanes (AFD) envisage de retirer des domaines essentiels de son activité de la loi sur la transparence. C'est ce qu'elle propose dans le projet de nouvelle loi fédérale sur la douane et la sécurité des frontières. Le Préposé, dans sa prise de position, s'est prononcé contre ces objectifs dans le cadre de la consultation des offices.

Dans le projet de loi sur la douanes et la sécurité des frontières, l'AFD a présenté des dispositions et des mesures visant à exclure de la loi sur la transparence des domaines essentiels de l'accomplissement de ses tâches publiques. L'AFD propose par exemple d'introduire une disposition permettant à l'autorité de collecter des données de particuliers fournies sur une base volontaire. Selon le rapport explicatif, ces données personnelles fournies « volontairement » devraient être soumises au secret spécifique prévu à l'art. 7, al. 1, let. h, LTrans. Plus précisément, ces données devraient être traitées afin de ménager aux opérateurs économiques des facilités de procédure supplémentaires.

Dans son avis, le Préposé a rappelé à l'AFD que trois conditions cumulatives devaient être remplies pour que l'exception mentionnée soit applicable. En premier lieu, l'information doit avoir été communiquée par un particulier. En second lieu, cette communication doit avoir été volontaire et spontanée. Il n'y a pas de caractère volontaire si l'information a été fournie dans le cadre d'une obligation légale ou contractuelle. Enfin, l'autorité doit avoir garanti le secret à la demande expresse de l'informateur. L'autorité ne peut ni offrir cette garantie de son propre chef ni la fournir à la légère. Étant donné les facilités procédurales supplémentaires que prévoit d'accorder l'AFD, le Préposé doute d'emblée de l'existence du critère de « caractère volontaire ». En outre, la garantie du secret ne peut être donnée qu'à la demande du particulier et uniquement dans des cas spécifiques. Il est impossible qu'une autorité donne une garantie proactive et générale, car le Conseil fédéral a lui-même explicitement déclaré dans son message relatif à la loi sur la transparence que dans le cas contraire, le but même de la loi, qui est de faciliter l'accès du public aux documents officiels et de promouvoir la transparence de l'administration, serait compromis.

La proposition de l'AFD va donc à l'encontre de l'esprit et du but de la loi sur la transparence et de la clause d'exception de l'art. 7, al. 1, let. h, LTrans.

De surcroît, le projet prévoyait une obligation de garder le secret, à l'égard d'autres autorités et des tiers, pour quiconque est chargé de l'exécution de la loi ou participe à son exécution sur les faits dont il a connaissance dans l'exercice de ses fonctions et de refuser la consultation des pièces officielles.. Selon l'AFD, cette large obligation de garder le secret devrait également valoir par analogie pour la loi sur l'imposition des véhicules automobiles, la loi sur l'imposition des huiles minérales et la loi sur l'alcool. Selon le rapport explicatif de l'AFD, de nombreuses demandes d'accès actuellement déposées ne portent pas sur les activités de l'administration, mais visent uniquement à obtenir des données économiques sensibles de tiers. L'AFD méconnaît ici que le législateur a déjà lui-même assuré la protection de « données économiques » sensibles dans la loi sur la transparence. Ainsi, les informations en question concernant les entreprises sont d'ores et déjà largement protégées par l'art. 7, al. 1, let. g, LTrans (secrets professionnels, d'affaires ou de fabrication). Les documents requis peuvent être caviardés s'il existe des preuves fondées de l'existence de ce type de secrets ou, s'il est impossible de les caviarder, ces documents peuvent être complètement soustraits à l'accès. Par ailleurs, les entreprises concernées peuvent intenter une action en justice pour se défendre contre l'octroi de l'accès tel qu'il est envisagé par l'administration. Il existe à cet égard une jurisprudence du Tribunal fédéral longue de plusieurs années.

En outre, avec cette vaste réserve relative au secret, l'AFD ignore la volonté claire du législateur selon laquelle la loi sur la transparence vise à promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration. Avec l'introduction du principe de la transparence, l'intention explicite du législateur était que la population dépose des demandes d'accès en particulier aussi pour contrôler les autorités dans leurs rapports avec des tiers. Le principe de la transparence vise donc également à prévenir la mauvaise gestion et la corruption dans l'administration. Indirectement, il protège aussi certains secteurs de l'administration fédérale contre les soupçons d'avoir conclu des accords secrets ou usé de pratiques déloyales avec des opérateurs économiques au détriment d'autrui ou aux dépens des contribuables.

Le Préposé a également rappelé à l'AFD que les demandes d'accès impopulaires ou les éventuelles charges de travail ne sont pas en soi des arguments valables et suffisants pour exiger une disposition supplémentaire garantissant le secret. Pour ces raisons, dans le cadre de la procédure de consultation, le Préposé a demandé à l'AFD de supprimer cette disposition anti-transparence sur l'obligation de garder le secret pour toutes les lois concernées.

Sur la base des réactions des autorités consultées, l'AFD a remanié son projet et procédé à une deuxième consultation des offices. Dans le projet de loi remanié, la disposition concernant l'obligation de garder le secret des personnes chargées de l'exécution de la loi a été supprimée et le rapport explicatif adapté à différents endroits. Néanmoins, pour le reste, l'AFD a campé sur sa position.

À la clôture de la rédaction, la décision du DFF sur la poursuite de la procédure était toujours attendue. Si le Conseil fédéral et le Parlement suivent l'avis de l'AFD, de larges pans des tâches principales incombant de par la loi à l'AFD ne seraient plus soumis au principe de la transparence

.

Les consultations relatives à la Convention entre la Confédération et les cantons sur l'harmonisation et la mise à disposition commune de la technique et de l'informatique policières en Suisse

Dans une convention passée entre la Confédération et les cantons sur l'harmonisation et la mise à disposition commune de la technique et de l'informatique policières en Suisse (CTIP Suisse), la Conférence des directrices et directeurs cantonaux de justice et police (CCDJP) a inclus une disposition sur le droit applicable, aux termes de laquelle le droit cantonal bernois, et non la loi fédérale sur la transparence, doit s'appliquer à la transparence de l'administration fédérale, dans le contexte de la technique et de l'informatique policières.

En 2010, la CCDJP a établi le Programme d'harmonisation de l'informatique policières (HIP). La mise en œuvre opérationnelle de ce programme a été confiée à un service sis auprès du Centre de compétence suisse de technique et d'informatique policières (TIP). Les deux domaines d'activité HIP et TIP devraient désormais être régis par une seule convention entre la Confédération et les cantons. Or dans le projet de cette convention figure une disposition sur le droit applicable selon laquelle seule la loi bernoise sur l'information de la population devrait être applicable (entre autres) à la transparence dans l'administration pour toutes les autorités cantonales et fédérales concernées.

Au début de l'année sous revue, dans le cadre d'une consultation préliminaire menée par l'Office fédéral de la justice OFJ, le Préposé avait déjà clairement précisé que la disposition proposée sur le droit applicable – pour ce qui concerne les autorités fédérales – contourne la loi fédérale sur la transparence et contrevient ainsi au droit fédéral, ce qui à son tour enfreint l'art. 48, al. 3, de la Constitution fédérale, selon lequel les accords entre cantons ne doivent être contraires ni aux droits ni aux intérêts de la Confédération, ni aux droits des autres cantons. Au cours d'une consultation ultérieure, le Préposé a rappelé à l'intention de la CCDJP que même si entre temps ses remarques transmises à l'OFJ avaient été intégrées aux commentaires explicatifs relatifs à la convention, la disposition sur le droit applicable demeurait inchangée dans le projet de convention. De ce fait, selon le libellé de cette disposition, le droit cantonal bernois continue de s'appliquer aux autorités fédérales parties à la convention, par exemple en ce qui concerne la transparence dans l'administration, à propos de questions relevant de la protection des données ou des marchés publics. Le Préposé a souligné à l'intention de la CCDJP que la réserve d'applicabilité de la loi fédérale sur la transparence pour les autorités fédérales doit figurer dans la convention même, surtout pour des raisons de sécurité du droit, et pas seulement dans les commentaires explicatifs qui, comme chacun sait, ne sont consultés que si une norme n'est pas claire.

Enfin, le Préposé a souligné qu'indépendamment de la participation d'une ou plusieurs autorités fédérales à la convention en question, ces autorités demeurent soumises à la loi fédérale sur la transparence si elles produisent des documents ou en reçoivent en tant que destinataires principales. En d'autres termes, cela signifie que pour les autorités fédérales, lors de l'examen des demandes d'accès aux documents officiels relatifs à l'harmonisation et à la mise à disposition commune de la technique et de l'informatique policières, ce n'est pas la loi cantonale bernoise sur l'information de la population qui est déterminante, mais uniquement la loi fédérale sur la transparence.

Consultation des offices relative au répertoire central des documents officiels

Les Archives fédérales suisses (AFS) ont demandé au Conseil fédéral de réaliser une étude en vue de fournir une base de décision concernant la création d'un répertoire central des documents officiels. Les précisions fournies par le Préposé ont été intégrées à la demande adressée au Conseil fédéral.

En 2008, le Conseil fédéral avait décidé d'introduire GEVER et de créer un répertoire central des documents officiels dans l'administration fédérale (répertoire appelé aussi « single point of orientation » ou SPO, point unique d'orientation). Le SPO devait utiliser les métadonnées du programme de gestion électronique des données GEVER pour créer un registre. Les résultats de la recherche dans ce répertoire central devaient également aider les demandeurs en vertu de la loi sur la transparence pour déposer des demandes d'accès précises. En 2012, les AFS ont développé et testé une application-pilote de recherche en ligne. Le projet a ensuite été suspendu à deux reprises. Fin 2019, les AFS devaient présenter au Conseil fédéral un récapitulatif de la situation et faire une proposition sur la suite à donner au projet. Dans le cadre d'une consultation des offices, le Préposé a pris position sur la proposition des AFS « Répertoire central des documents officiels ».

Un « répertoire central des documents officiels », méta-informations comprises, servirait à mettre en œuvre le principe de la transparence et contribuerait à rendre l'administration plus transparente. Le Préposé salue d'ailleurs ces efforts. Dans sa prise de position transmise aux AFS, il a souligné l'importance de faire une nette distinction, au sein du projet « Répertoire central des documents officiels », entre la loi sur la transparence et le mandat général d'information des autorités. Certes l'art. 21 LTrans contient une disposition d'exécution relative à l'information sur les documents officiels. Toutefois, cela ne crée pas une base légale distincte, mais précise seulement l'obligation générale d'information, déjà existante, des autorités.

Un « répertoire central des documents officiels » est un instrument de l'information active des autorités publiques : selon la Constitution et la loi sur l'organisation du gouvernement et de l'administration, les autorités publiques ont d'ores et déjà le devoir général de transmettre de leur propre chef des informations sur leurs tâches et leurs affaires importantes, et de fournir à cet effet des informations adéquates (information active). En revanche, la loi sur la transparence s'applique lorsqu'une personne présente une demande d'accès à une autorité (information passive).

Lors de sa séance du 6 décembre 2019, le Conseil fédéral a décidé de réaliser une étude sur la création d'un répertoire central des documents officiels. La manière de mettre en œuvre ce type d'instrument, les solutions techniques ainsi que les compétences au sein de l'administration fédérale devront entre autres être clarifiées. Les Archives fédérales présenteront les résultats de cette étude d'ici la fin de l'année 2020.

Consultation des offices relative à la convention tarifaire Thérapie cellulaire CAR-T

Au moyen d'une décision du Conseil fédéral, l'Office fédéral de la santé publique (OFSP) voulait exclure la convention tarifaire concernant les thérapies cellulaires autologues CAR-T de la loi sur la transparence. Le Préposé s'est prononcé contre cette manière de procéder.

L'OFSP proposait au Conseil fédéral d'approuver la convention tarifaire entre les hôpitaux et les assurances-maladies (partenaires contractuels) concernant le traitement de la thérapie cellulaire autologue CAR-T. Cette convention contient un accord de confidentialité selon lequel les niveaux de rémunération contractuels variables pour les transplantations autologues de cellules CAR-T ne peuvent être accessibles, outre les parties contractantes, qu'aux autorités d'approbation et aux autorités sanitaires compétentes du canton de résidence du patient. L'OFSP faisait valoir, entre autres, que le montant de la rémunération constituait un secret d'affaires. Il suggérait par ailleurs que la proposition au Conseil fédéral et les conventions de rémunération énumérés en annexe restent exclues du droit d'accès prévu par la loi sur la transparence, même après l'approbation de la convention tarifaire par le Conseil fédéral.

.

Dans le cadre de la consultation des offices, le Préposé a relevé en premier lieu à l'intention de l'OFSP que dans le domaine de l'assurance obligatoire, les assureurs-maladie et les assureurs-accidents sont considérés comme des autorités au sens de la loi sur la transparence. Les informations fournies à l'OFSP par des tiers à des fins d'approbation des tarifs sont fondées sur des exigences légales (loi fédérale sur l'assurance-maladie), raison pour laquelle un accord de confidentialité dans le cadre d'une convention tarifaire ne peut être ni valablement convenu, ni approuvé par le Conseil fédéral. En outre, le Préposé a souligné que la loi sur la transparence garantit déjà à la fois la protection du secret d'affaires et la protection de la sphère privée, raison pour laquelle une exception à la loi sur la transparence n'est pas nécessaire. Il a poursuivi en indiquant que la proposition au Conseil fédéral signée fait partie de la procédure de co-rapport et qu'elle est donc d'emblée exclue, en vertu de l'art. 8, al. 1, LTrans, du droit d'accès prévu par la loi sur la transparence, contrairement aux annexes qui y sont jointes.

Par souci d'exhaustivité, le Préposé a également précisé qu'il ne s'agit pas ici d'un cas d'application de l'art. 8, al. 3, LTrans car la convention tarifaire et les accords de rémunération qui y sont associés ont été établis avant le début de la procédure de consultation des offices et ne sont donc pas considérés comme des documents officiels de cette procédure (le Préposé a déjà commenté cette question dans son 26e Rapport d'activités, ch. 2.4).

Selon l'art. 8 al. 3, LTrans, le Conseil fédéral peut exceptionnellement et définitivement exclure de l'accès les documents officiels de la procédure de consultation des offices après la prise de décision. Toutefois, dans son appréciation, il doit être guidé par les exceptions prévues dans la loi sur la transparence.

Le Préposé a en particulier attiré l'attention de l'OFSP sur le fait que la loi sur la transparence ne permet pas au Conseil fédéral d'exclure des documents officiels du champ d'application de la loi sur la transparence sur la base d'une décision, limitant par là-même le champ d'application de la loi sur la transparence, selon sa propre volonté et appréciation en contournant ainsi le processus législatif ordinaire.

À la suite de cela, l'OFSP a ensuite modifié la proposition au Conseil fédéral. Cependant, à peine quelques semaines plus tard, il relançait la demande d'une d'exclure un domaine de la loi sur la transparence et proposait une révision partielle dans ce sens de la loi sur l'assurance-maladie (cf. texte ci-après).

Procédure de consultation des offices sur la révision partielle de la LAMal concernant les mesures visant à maîtriser les coûts – Second volet

Le Préposé s'est prononcé contre l'intention du Conseil fédéral d'introduire une exception au principe de la transparence pour les documents relatifs aux modèles de prix des médicaments dans l'assurance-maladie.

Dans le cadre d'une consultation des offices, l'Office fédéral de la santé publique (OFSP) a proposé entre autres une exception à l'accessibilité des documents concernant le montant, le calcul et les modalités dans le cadre de modèles de prix et de remboursements dans l'assurance-maladie obligatoire. Lors de la fixation du prix des médicaments figurant sur la liste des spécialités (LS), des rabais (appelés modèles de prix) peuvent être négociés entre les entités pharmaceutiques en tant que titulaires d'autorisation et les assureurs-maladie. Dans ces modèles de prix, le prix officiel figurant sur la LS diffère du prix réel que l'assureur-maladie doit payer à la société pharmaceutique (remboursement).

Par cette proposition, le Conseil fédéral entend exclure du champ d'application de la loi sur la transparence tous les documents relatifs aux modèles de prix. Les rabais convenus et la totalité du mécanisme de remboursement ne doivent pas être portés à la connaissance du public. Le Conseil fédéral est d'avis que si les prix réels étaient dévoilés, les entreprises pharmaceutiques ne seraient plus disposées à négocier ces modèles de prix.

Le Conseil fédéral fait également valoir que la majorité des demandes d'accès en lien avec des documents relatifs aux médicaments figurant sur la liste des spécialités ne sont pas présentées par des citoyens souhaitant obtenir des informations sur l'activité de l'État, mais surtout par des entreprises pharmaceutiques désirant accéder aux informations commerciales d'entreprises concurrentes. À cela, il convient d'objecter que les concurrents ont également un intérêt légitime à pouvoir contrôler la pratique de l'OFSP en matière d'autorisations pour les produits concurrents. Les secrets d'affaires et de fabrication ainsi que la sphère privée des entreprises concernées restent explicitement protégés même lorsque la loi sur la transparence est appliquée.

De l'avis du Préposé, l'introduction d'une disposition sur le maintien du secret dans la loi sur l'assurance-maladie ne va pas dans le bon sens. Dans le cadre de la consultation des offices, il a rappelé que le principe de la transparence vise à promouvoir la compréhension de l'administration et de son fonctionnement ainsi qu'à accroître l'acceptation de l'action étatique. L'utilisation de ces modèles de prix par l'OFSP est un instrument de politique des prix de plus en plus utilisé. À l'inverse, il existe un large consensus en faveur de la transparence des coûts dans le domaine de la santé, d'autant plus que la population désigne depuis des années l'augmentation continue des primes d'assurance-maladie comme l'une de ses plus grandes préoccupations.

Dans ce contexte, il est essentiel que la population et les concurrents conservent la possibilité de comprendre et contrôler de manière exhaustive la pratique d'autorisation de l'OFSP. À moyen et long terme, une stratégie de transparence active, en particulier au niveau international, permettrait de diminuer les prix. Une coopération étroite entre les États est essentielle pour une politique des prix réellement efficace à long terme.

L'OFSP n'a pas tenu compte des préoccupations du Préposé. Le Conseil fédéral ouvrira prochainement une procédure de consultation concernant une révision partielle de la loi sur l'assurance-maladie.

Consultation des offices sur la révision totale de l'ordonnance sur les marchés publics

Au cours des travaux pour la révision totale de l'ordonnance sur les marchés publics, une divergence est apparue entre le Préposé et le Conseil fédéral à propos de l'accessibilité de la nouvelle liste des soumissionnaires sanctionnés.

Le 21 juin 2019, le Parlement a adopté la révision totale de la loi fédérale sur les marchés publics (LMP) (numéro d'objet parlementaire 17.019). Contrairement au projet d'exemption totale du Conseil fédéral, le principe de la transparence dans le domaine des marchés publics demeure dans le nouveau projet de loi – comme c'est déjà le cas dans la LMP actuelle.

Le Préposé s'était résolument prononcé dans ce sens au cours de la procédure de consultation des offices et durant les débats parlementaires (cf. 26e Rapport d'activités 2018/19, ch. 2.4). Dans la première partie de l'année sous revue, l'OFCL a présenté le projet d'ordonnance entièrement révisée dans le cadre d'une procédure de consultation. L'art. 45, al. 3, de la loi adoptée par le Parlement a introduit une liste de soumissionnaires et des sous-traitants sanctionnés, désignée comme « non publique ».

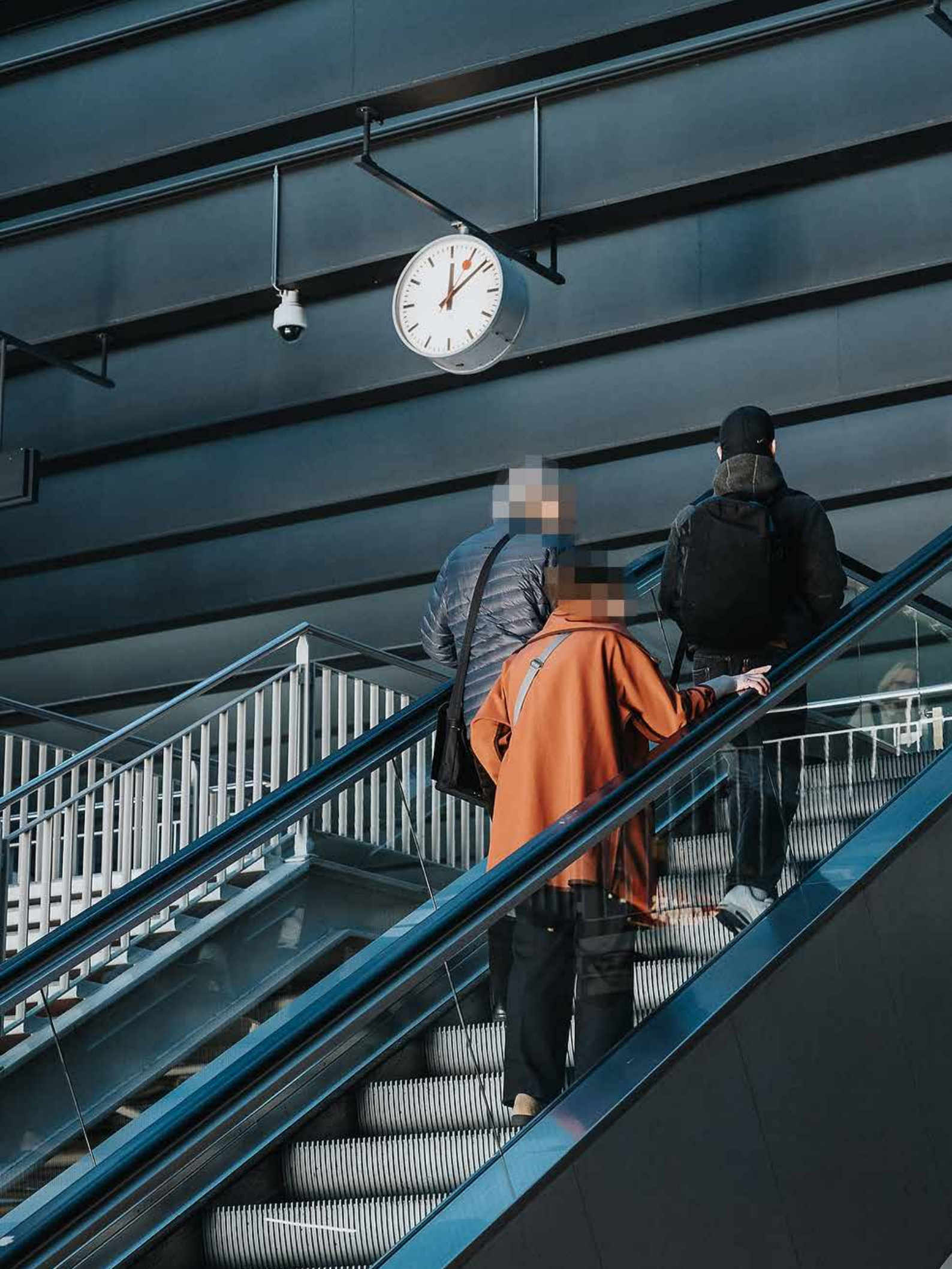
Cette liste répertorie les entreprises contre lesquelles une exclusion, entrée en force, des futurs marchés publics a été prononcée, par exemple parce qu'elles ont enfreint les dispositions relatives à la lutte contre la corruption ou ont conclu des accords illicites affectant la concurrence. L'art. 25, al. 3, de l'ordonnance révisée prévoit un droit à part d'accès à cette liste uniquement pour les entités adjudicatrices, mais pas un droit général d'accès du public. Dans le rapport explicatif de l'ordonnance sur les marchés publics, il est précisé que, selon le message relatif à la LMP, il n'existe aucun droit d'accès en vertu de la loi sur la transparence.

Dans le cadre de la consultation des offices, le Préposé s'est exprimé contre cette interprétation : dans le projet du Conseil fédéral relatif à la révision de la LMP, tous les documents relatifs aux marchés publics étaient complètement exclus du champ d'application de la loi sur la transparence. Or le Parlement s'est prononcé en faveur d'une transparence totale des marchés publics et a rejeté les intentions de secret du Conseil fédéral. Conformément à la volonté claire de transparence du législateur, la loi sur la transparence doit donc s'appliquer sans restriction aucune à la loi fédérale révisée sur les marchés publics.

Par ailleurs, le Préposé estime que la simple désignation de la liste dans la loi comme « non publique » ne suffit pas pour la qualifier de « secrète » au sens d'une disposition spéciale de l'art. 4, LTrans. Il faudrait pour cela une réserve légale formelle et explicite à la loi sur la transparence dans la LMP même. « Non publique » signifie en fait simplement que la liste n'est pas activement publiée par les autorités. Le libellé de la disposition légale n'implique en aucune façon que la liste doit être tenue secrète face à une demande d'accès.

Cette divergence n'a pas pu être levée. Le Conseil fédéral a rejeté les objections du Préposé.

La loi révisée et l'ordonnance y relative entreront en vigueur le 1er janvier 2021.



Le PFPDT

3.1 Tâches et ressources

Le Préposé

Lors de sa séance du 10 avril 2019, le Conseil fédéral a réélu Adrian Lobsiger pour un second mandat (51e législature) qui durera jusqu'à la fin de l'année 2023.

Prestations et ressources dans le domaine de la protection des données

Effectifs

De 2005 à 2019, le nombre des collaborateurs affectés à l'application de la loi sur la protection des données (LPD) a fluctué entre 20 et 24 postes à plein temps. Ces fluctuations s'expliquent d'une part par le fait que la loi sur la transparence (LTrans) est entrée en vigueur en 2006. Les postes prévus à cet effet n'ayant jamais été approuvés par le Conseil fédéral, notre autorité a dû recourir au personnel existant du PFPDT et, dans certains cas, a mobilisé les moyens de la Chancellerie fédérale. D'autre part, les postes supplémentaires accordés dans le contexte de l'adhésion aux accords de Schengen et de Dublin ainsi que de l'édiction de lois spéciales dans le secteur de la santé n'ont jamais pu être entièrement pourvus en raison de mesures générales d'économie.

Dans son message concernant la révision totale de la LPD, le Conseil fédéral a prévu pour le Préposé la création de neuf à dix postes supplémentaires (FF 2017 6784). Entre-temps, 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). La

LPDS confie à nos autorités des tâches et compétences supplémentaires en ce qui concerne le traitement particulièrement sensible des données personnelles dans le domaine de la police (cf. 26e Rapport, , ch. 1.2).

Après avoir fait entrer cette loi en vigueur au 1er mars 2019, le Conseil fédéral a attribué au Préposé trois postes supplémentaires pour la mise en œuvre des nouvelles tâches et compétences. C'était la première fois depuis 2005 que le budget consacré au personnel chargé de la protection des données augmentait. Au printemps 2020, ces trois postes supplémentaires étaient pourvus, de sorte que les effectifs du PFPDT s'élèvent désormais à 27 postes à plein temps. En raison du champ d'application étroit de la LPDS, le personnel supplémentaire sera principalement affecté à la surveillance des autorités de police fédérales. À la suite de plusieurs départs, la structure d'âge de notre personnel a baissé, ce qui allégera la charge pesant sur les dépenses en personnel et permettra probablement une augmentation supplémentaire de nos effectifs au cours de la prochaine période de référence.

Quant à savoir quand le Préposé pourra demander et recruter le personnel supplémentaire prévu pour la mise en œuvre de la révision totale, cela dépend de la date, encore incertaine, d'entrée en vigueur de la nouvelle LPD. Conformément à l'art. 40a du projet de loi, approuvé par les deux Chambres fédérales, le Préposé ne transmettra son projet de budget au Conseil fédéral qu'au printemps suivant l'entrée en vigueur de la loi. De quel printemps s'agira-t-il, nous ne le savons pas encore. Le Conseil fédéral soumettra ensuite le projet inchangé à l'Assemblée fédérale, qui décidera jusqu'à l'hiver suivant si et dans quelle mesure elle augmentera notre budget.

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

2005	22
2010	23
2018	24
2019	24
2020	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 2019 au 31 mars 2020, les ressources en personnel dont dispose le Préposé pour la protection des données ont été réparties comme suit (cf. Tab. 5) :

Tableau 5 : Prestations en matière de protection des données

Conseil Privés	16,5%	
Conseil Confédération	18,8%	
Collaboration avec les cantons	2,5%	
Collaboration avec des autorités étrangères	12%	
Total Conseil		**49,8%**
Surveillance	16%	
Certification	0,1%	
Registre de données	0,6%	
Total Surveillance		**16,7%**
Information	18,7%	
Formation/Conférences	5,5%	
Total Information		**24,2%**
Législation	9,3%	
Total Législation		**9,3%**
Total Datenschutz		**100%**

Conseil

Comme indiqué dans le chapitre introductif « Défis actuels et priorités », le Préposé est confronté à une demande croissante de prestations de conseil en raison de la nécessité de suivre les projets numériques d'envergure. Comme nous devons élargir nos activités de surveillance, les ressources en personnel consacrées au conseil ont été réduites d'environ 4 %, pour atteindre 49,8 %. Selon le planning de contrôle du Préposé pour l'année 2020, le suivi de douze grands projets est en cours. Ses ressources n'étant encore adaptées ni aux risques technologiques accrus de ré-identification, ni aux transmissions non autorisées de données , ni aux autres défis de la numérisation, le Préposé n'est toujours pas en mesure de répondre à la demande croissante de suivi de projets de conseil dans les détails et les délais souhaités. Au cours de la période sous revue, les trois unités du domaine de direction de la protection des données ont répondu mensuellement à environ 65 demandes et signalements de citoyens et citoyennes, par des lettres-types les réorientant vers les voies civiles.

Cette situation se traduit par une incompréhension croissante, d'une part car le Règlement général sur la protection des données de l'Union européenne oblige les autorités de protection des données à donner suite à toutes les plaintes des citoyens, d'autre part car le projet de révision totale de la LPD prévoit également pour le PFPDT une obligation élargie visant à traiter matériellement les préoccupations individuelles de la population suisse.

De plus, notre autorité a dû réduire ses activités de conseil dans d'autres domaines tels que la coopération internationale. Étant donné que le « Big Data » et l'intelligence artificielle s'imposent comme modèles économiques dans des secteurs toujours plus nombreux et que les risques pour la protection des données en relation avec ces développements technologiques élargissent encore le domaine de surveillance du PFPDT, on peut, comme pour les années précédentes, s'attendre à ce que le nombre de grands projets de traitement de données dans l'administration et l'économie continue à augmenter.

Tableau 6 : Activité de conseil sur des grands projets en 2019

Droits fondamentaux	1
Transports	1
Finances	1
Santé et Secteur de travail	3
Sécurité	2
Télécommunication	1
Médias	1
Commerce et économie	2
Total	**12**

Surveillance

En raison de la dynamique des applications basées sur le cloud, les contrôles doivent aujourd'hui être effectués rapidement. Cette accélération, ainsi que la combinaison de plus en plus importante de compétences juridiques et techniques, excluent toute longue interruption dans les procédures d'établissement des faits, si bien que les contrôles d'envergure doivent être suivis par plusieurs collaborateurs. Les effectifs actuels restreignent considérablement la densité des contrôles. En 2018, environ 12 % des ressources en personnel ont été affectées aux activités de surveillance, ce qui est nettement inférieur à la moyenne à long terme d'environ 20 %. Au cours des deux dernières périodes, cette proportion a de nouveau augmenté pour atteindre environ 17 %. Selon le planning de contrôle pour 2020, ces ressources seront utilisées pour effectuer quinze contrôles plus complets. Par rapport aux quelque 12 000 grandes et moyennes entreprises commerciales et 100 000 fondations et associations en Suisse, la densité actuelle des contrôles est encore faible. Il reste difficile pour le Préposé de faire part aux médias et aux organisations de protection des consommateurs de sa réticence à ouvrir des procédures d'établissement des faits en raison des ressources restreintes dont il dispose. augmenter.

Législation

L'évolution technologique qualifiée de « fulgurante » par le Conseil fédéral dans l'introduction de son message sur la révision totale de la LPD (FF 2017 6567) se reflète également dans le traitement des données personnelles par les organes fédéraux, autorisé uniquement en présence de bases légales. Il en résulte un grand nombre de nouvelles dispositions dans le droit fédéral, sur lesquelles le Préposé doit se prononcer dans le cadre de diverses procédures de consultation.

Les interventions dans ce domaine ont fortement augmenté au cours des dix dernières années, ce qui contribue également à une baisse de la densité des contrôles. Néanmoins, nous avons réussi à stopper cette tendance au cours de l'avant-dernière période sous revue. Compte tenu de nos ressources limitées, nous sommes contraints de motiver de manière sommaire nos prises de position dans le cadre des consultations et de réduire nos prestations dans d'autres domaines.

Révision totale de la LPD

Comme nous l'avons déjà mentionné dans le précédent rapport d'activités, des instruments de travail modernes – tels que l'analyse d'impact relative à la protection des données - ont vu le jour dans la pratique de la réalité numérique. Ils font désormais partie du quotidien de notre autorité dans la gestion des grands projets numériques (cf. Tab. 6).

Pour une consolidation juridiquement sûre de ces instruments de travail et des activités de surveillance du Préposé en la matière, il est indispensable qu'ils soient inscrits non seulement dans le RGPD, mais aussi dans le droit suisse de la protection des données, ainsi que le prévoit la révision totale de la LPD. Comme nous ne pouvons toujours pas dire quand la nouvelle LPD entrera en vigueur, notre autorité doit mettre en œuvre ces nouveaux instruments de travail de manière pragmatique avec les ressources en personnel dont elle dispose actuellement.

Participation aux délibérations de commissions et auditions par les Commissions parlementaires

À l'occasion de la visite dans nos bureaux de la sous-commission DFJP/ChF de la Commission de gestion du Conseil des États (CdG-E) en 2018, nous avons présenté les résultats de l'essai-pilote « Procédure de médiation accélérée ». Puis, lors d'une audience tenue en avril 2019, nous avons informé la sous-commission du passage réussi du projet-pilote au fonctionnement ordinaire.

Au cours de la période sous revue, d'autres auditions ont porté sur l'utilisation systématique du numéro d'AVS par les autorités (modification de la LAVS) en février 2020 au sein de la Commission des institutions politiques du Conseil des États (CIP-E) et en octobre 2019 par la sous-commission DFI/DETEC de la CdG-N sur le dossier électronique du patient (DEP). En avril et mai 2019, nous avons également participé aux délibérations de la Commission des affaires juridiques du Conseil des États (CAJ-E) concernant la loi fédérale sur les services d'identification électronique.

Critères de calculs

La question de savoir si et dans quelle mesure des ressources seront allouées au PFPDT relève de la responsabilité des autorités politiques ; celles-ci disposent d'une latitude considérable pour évaluer les développements actuels et futurs de la numérisation et leur impact sur les activités de notre autorité. La tâche principale du Préposé est de protéger la sphère privée et de garantir le droit à l'autodétermination informationnelle dans la société numérique. Il doit pouvoir agir en toute indépendance.

Cela nécessite des ressources humaines, matérielles, techniques et financières appropriées et suffisantes, qui ne limitent pas l'autorité de contrôle à faire ce qui est indispensable de manière réactive, mais lui permettent de prendre l'initiative d'agir – avec un degré de crédibilité et d'intensité que le public concerné peut raisonnablement attendre afin que ses droits fondamentaux soient protégés.

Les objectifs de résultats, servant de base au calcul des ressources, ont donc été définis en fonction des différents groupes de prestations comme suit (cf. Tab. 7) :

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

Le domaine de direction « Principe de la transparence », qui continue d'employer 3,6 personnes, est passé à une procédure accélérée et sommaire en 2017 après un essai d'un an ; d'une manière générale, les procédures de médiation sont donc désormais menées oralement.

Ce type de procédure continue à faire ses preuves, car la proportion de médiations abouties reste élevée et le dépassement des délais légaux a été généralement limité aux affaires complexes tant sur le plan de la procédure que du contenu. Toutefois, l'année en cours a également montré que l'augmentation du nombre de demandes en médiation, le dépôt de nombreuses demandes en un court laps de temps et les vacances de postes entraînent rapidement des cumuls de retard, avec pour conséquence que les délais légaux pour la conduite des procédures de médiation ne peuvent plus être respectés (cf. ch. 2.3).

Si la tendance à l'augmentation du nombre de demandes (complexes) en médiation se poursuit, les retards dans le traitement des procédures risquent d'avoir un impact négatif sur les nouveaux dossiers ouverts.

Tableau 7 : Critères de calculs PFPDT

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

3.2 Communication

Augmentation des ressources due à des tâches supplémentaires et à un défaut de taille critique

Notre autorité s'efforce d'informer efficacement les médias et le grand public sur les questions touchant à la sphère privée et à la transparence dans l'administration. Pour ce faire, nous utilisons notre site Internet comme premier canal de communication : il est visité par environ 2000 personnes par jour. Au cours de l'année sous revue, le Parlement fédéral a poursuivi les débats relatifs à la révision totale de la loi sur la protection des données. Son entrée en vigueur accroîtra encore le besoin d'information de la population, des entreprises et des autorités.

Doté d'un poste et demi à plein temps, le service chargé de la communication, a dû également au cours de l'année sous revue, se concentrer sur le suivi médiatique de nos principales activités. Comme la LPD révisée prévoit de nouvelles obligations pour les entreprises et des tâches et pouvoirs supplémentaires pour notre autorité, le service de communication doit être élargi à deux postes et demi à plein temps, ce qui améliorera également son accessibilité. Le poste à pourvoir pourrait être mis au concours avant la fin de la période sous revue.

Il s'agira en premier lieu d'accompagner, sur le plan de la communication, la nouvelle loi révisée et de prendre les mesures appropriées pour informer et sensibiliser l'opinion publique. Cela inclut également les contenus cross-média et les formats audiovisuels. Toutefois, la première priorité est de revoir et de remanier nos feuillets thématiques, commentaires explicatifs et guides, en les adaptant aux nouvelles dispositions légales et ordonnances et de créer de nouvelles lignes directrices.

Grand intérêt des médias – en Suisse, mais aussi à l'étranger

L'intérêt du public pour la protection des données au travers des médias n'a cessé de croître ; du fait de notre compétence en matière de surveillance dans l'affaire du projet Libra, de plus en plus de médias étrangers se sont adressés au Préposé et nos échanges avec les autorités internationales de protection des données se sont intensifiés. La présence de ce thème dans la presse s'est traduite par de nombreuses déclarations du Préposé – en particulier par une présence parfois forte sur les chaînes de télévision. Dans les médias observés (presse écrite, radio, télévision), environ 2000 comptes rendus et articles sont parus, portant principalement sur des questions de protection des données, mais aussi de transparence dans l'administration. L'observation des principaux médias sociaux et plateformes en ligne a permis de répertorier environ 8800 mentions du Préposé ou de ses porte-parole – soit deux fois plus qu'en 2018, et avec un niveau d'activité très élevé dans le monde anglophone principalement dû au projet Libra. Au total, nous avons traité quelque 450 demandes de renseignements émanant des médias.

Les citoyens et les entreprises nous ont contactés par courrier électronique, par courrier postal ou ont choisi le service d'assistance téléphonique pour nous communiquer leurs préoccupations et transmettre leurs questions à nos spécialistes – un total d'environ 3000 demandes nous sont parvenues par ces canaux.

Le Préposé a également participé à une quarantaine d'événements en tant qu'intervenant à des conférences ou des tables rondes. Parmi les organisateurs de ces manifestations se trouvaient des associations, des sociétés, des établissements de formation, des autorités et des entreprises ainsi que des organismes actifs dans le numérique. Le Préposé a également participé aux discussions organisées au cours de la troisième Journée suisse du Digital et insisté sur la nécessité de sensibiliser le public sur les questions de protection de la sphère privée en intervenant dans des revues professionnelles à fort tirage, ciblées par exemple sur les transports, la finance ou la santé.

Communication conjointe des autorités fédérales et cantonales de protection des données à l'occasion de la Journée internationale de la protection des données

Depuis 2007, la Journée internationale de la protection des données se tient le 28 janvier de chaque année à l'initiative du Conseil de l'Europe. Son objectif est de sensibiliser les citoyens sur l'importance de la protection de la sphère privée et du droit à l'autodétermination informationnelle ; elle vise aussi à initier un changement durable des comportements à l'égard des nouvelles technologies.

En janvier 2020, le Préposé fédéral et les autorités cantonales de protection des données ont conjointement informé les médias sur les menaces croissantes auxquelles est exposée la sphère privée dans le domaine des transports privés et publics. Les risques en matière de protection des données découlent notamment de la surveillance au moyen d'enregistrements vidéo et de la création de profils de mouvements, qui s'imposent ou se sont imposés dans la vie quotidienne grâce au développement continuel de nouvelles applications de mobilité et des voitures connectées.

Prises de position, recommandations et publications

Au cours de la période sous revue, le Préposé a publié diverses déclarations et prises de position sur des projets ou des événements d'actualité, notamment sur les sujets suivants :

- l'association Libra, basée à Genève, qui a annoncé en juillet 2019 qu'elle avait lancé un projet de monnaie cryptographique mondiale ;
- l'application américaine Clearview qui, comme cela a été annoncé en janvier 2020, siphonne et commercialise des masses de données faciales provenant de sources accessibles au public ;
- les fonctionnalités de Facebook utilisées lors des élections fédérales d'octobre 2019 en Suisse ;
- les conséquences du Brexit dans le domaine des flux transfrontières de données pour la Suisse à partir du 31 janvier 2020 ;
- l'inégalité de traitement des citoyens suisses par rapport aux citoyens de l'UE par Postfinance qui utilise les empreintes vocales dans ses centres d'appel ;
- dans le cadre de la crise du coronavirus, l'application de traçage de proximité, l'accès de l'OFSP aux données de localisation de Swisscom ou encore l'utilisation des outils de vidéoconférence.

Nous avons également publié sur le site du Préposé 23 recommandations consacrées au principe de la transparence.

La plateforme interactive Think Data, reliée à notre site Internet, nous a permis de sensibiliser un large public à une meilleure protection des données et une meilleure transparence. Des recommandations en matière de protection des données sont formulées sur la base de scénarios concrets. Think Data est le projet du groupe de travail interdisciplinaire Think Services que le Préposé a contribué à mettre en place et continue de soutenir.

Comme l'année précédente, le rapport d'activités annuel est publié en quatre langues – à la fois en version imprimée et sous forme de document électronique dont le lien se trouve sur notre site Internet.

Le site Internet reste notre principal vecteur de communication

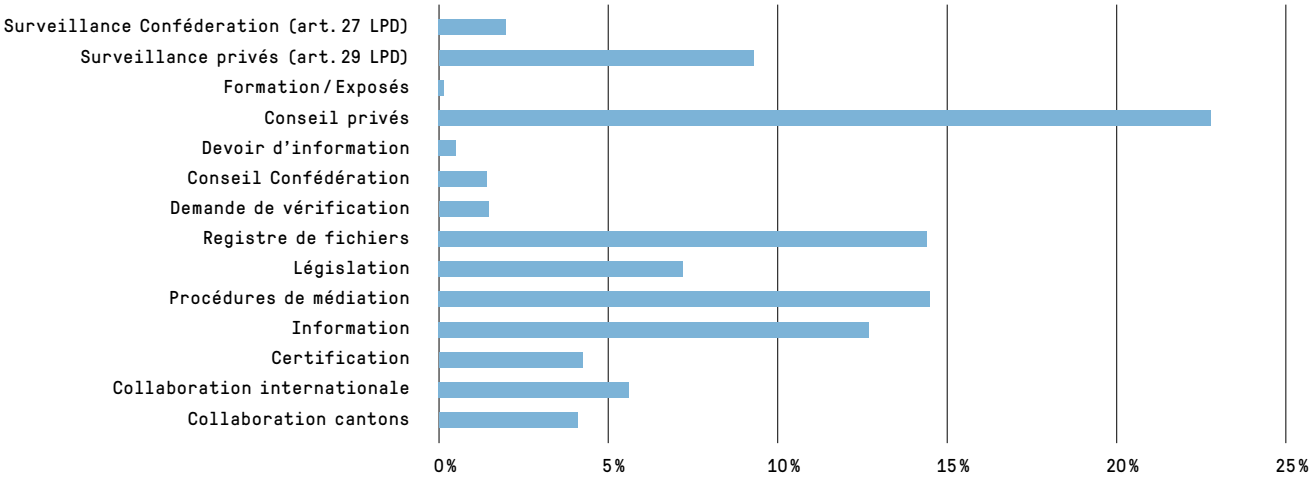
Le site Internet est le premier canal de communication du Préposé. Nous comptons presqu'un demi-million de visiteurs par an, soit environ 2000 par jour ouvrable. Deux visiteurs sur cinq viennent de l'étranger, principalement de pays européens, mais aussi d'outremer ou d'Asie. Les contenus sont généralement disponibles en trois langues : allemand, français et italien. Certains textes spécifiques sont également publiés en anglais pour les utilisateurs étrangers. Le site est optimisé étape par étape.

Nous informons également sur @derBeauftragte via Twitter, l'objectif étant de faciliter un accès rapide aux informations pertinentes pour nos abonnés et d'autres personnes intéressées par la protection des données. Dans un contexte de ressources limitées, mais aussi pour d'autres raisons, notre autorité a renoncé à l'utilisation d'autres réseaux sociaux.

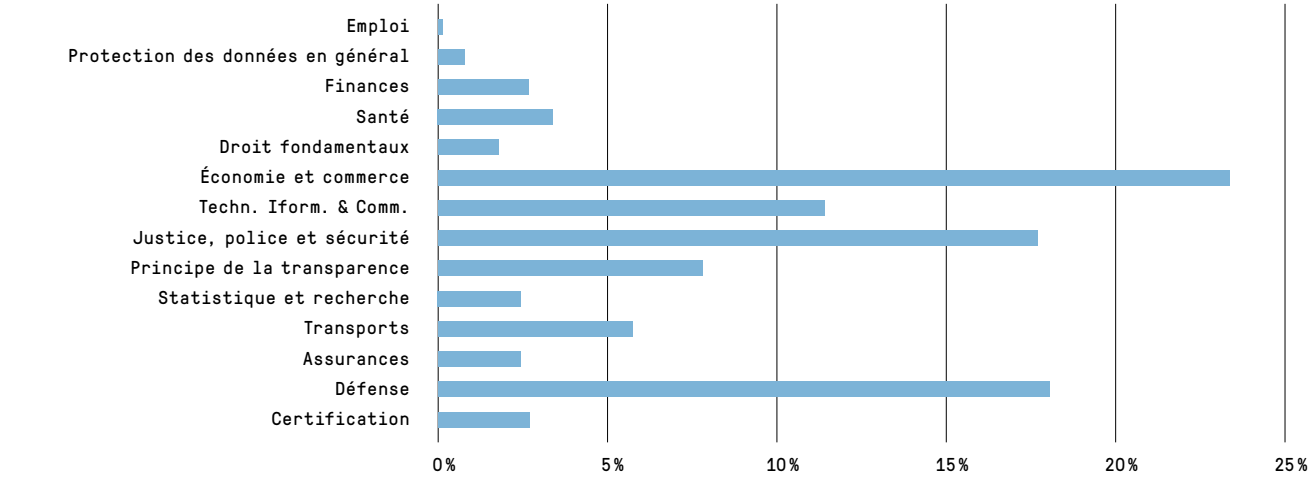
3.3 Statistiques

Statistiques des activités du PFPDT du 1er avril 2019 au 31 mars 2020 (Protection des données)

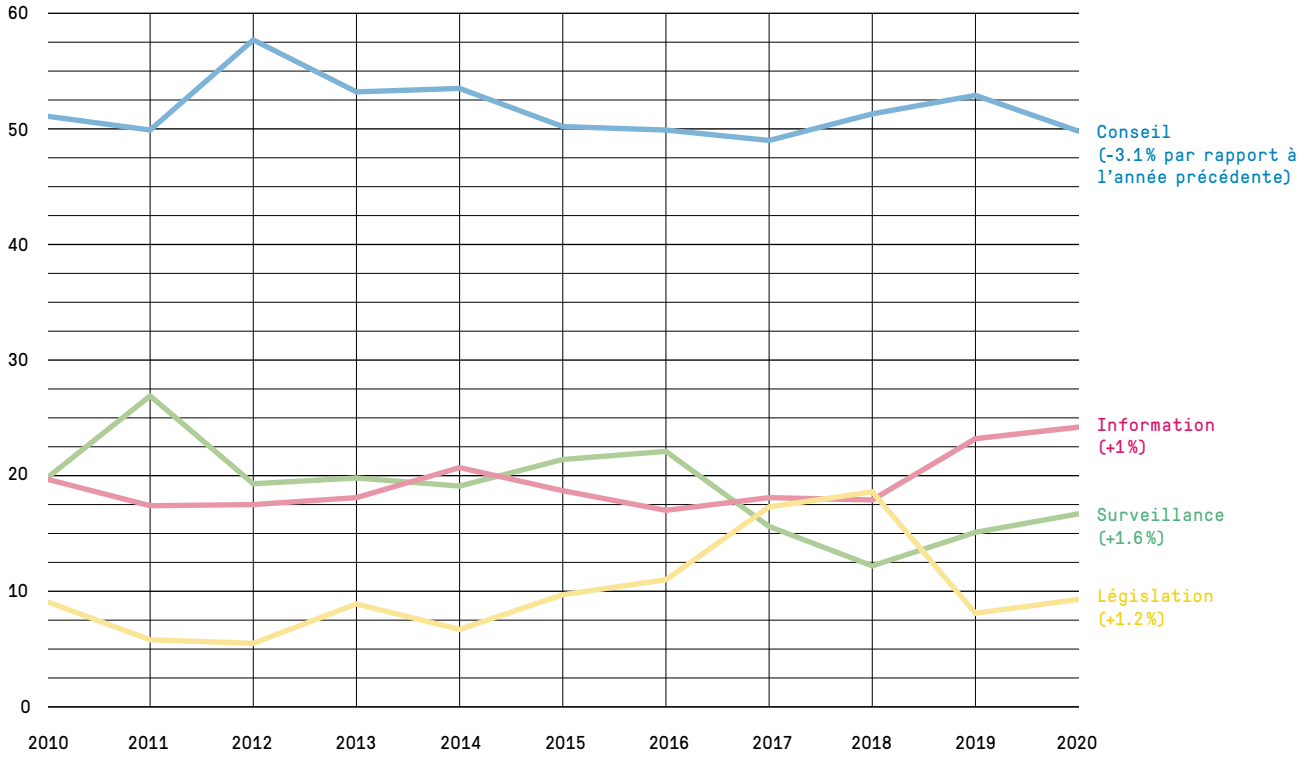
Charge de travail par tâches



Charge de travail par domaines



Comparaison pluriannuelle (en pourcentage)



Vue d'ensemble des demandes d'accès du 1er janvier 2019 au 31 décembre 2019

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	24		12		3		2		4		0		3	
DFAE	168		89		15		38		7		10		9	
DFI	126		52		15		31		8		9		11	
DFJP	48		27		8		9		2		1		1	
DDPS	225		193		6		14		6		4		2	
DFF	102		49		17		25		2		4		5	
DEFR	100		50		11		27		3		7		2	
DETEC	112		67		9		25		3		7		1	
MPC	10		3		1		0		3		1		2	
SP	1		0		1		0		0		0		0	
Total 2019 (%)	916	(100)	542	(59)	86	(9)	171	(19)	38	(4)	43	(5)	36	(4)
Total 2018 (%)	636	(100)	352	(55)	62	(10)	119	(19)	24	(4)	48	(7)	31	(5)
Total 2017 (%)	581	(99)	317	(55)	107	(18)	106	(18)	26	(4)	21	(4)	–	
Total 2016 (%)	551	(99)	293	(53)	87	(16)	105	(19)	33	(6)	29	(5)	–	
Total 2015 (%)	597	(100)	319	(53)	98	(16)	127	(21)	31	(5)	22	(4)	–	
Total 2014 (%)	575	(100)	297	(52)	122	(21)	124	(22)	15	(3)	17	(3)	–	
Total 2013 (%)	469	(100)	218	(46)	122	(26)	103	(22)	18	(4)	8	(2)	–	
Total 2012 (%)	506	(100)	223	(44)	138	(27)	120	(24)	19	(4)	6	(1)	–	
Total 2011 (%)	466	(100)	203	(44)	126	(27)	128	(27)	0	(0)	9	(2)	–	
Total 2010 (%)	239	(100)	106	(44)	62	(26)	63	(26)	0	(0)	8	(3)	–	

Statistique des demandes d'accès selon la loi sur la transparence du 1er janvier 2019 au 31 décembre 2019

	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	**14**	6	3	2	1	0	2
	PFPDT	**10**	6	0	0	3	0	1
	Total	**24**	**12**	**3**	**2**	**4**	**0**	**3**
Département fédéral des affaires étrangères DFAE	DFAE	**168**	89	15	38	7	10	9
	Total	**168**	**89**	**15**	**38**	**7**	**10**	**9**
Département fédéral de l'interieur DFI	SG DFI	**8**	3	2	3	0	0	0
	BFEG	**3**	2	0	0	0	0	1
	OFC	**4**	3	0	1	0	0	0
	AFS	**2**	2	0	0	0	0	0
	MétéoSuisse	**1**	1	0	0	0	0	0
	BN	**0**	0	0	0	0	0	0
	OFSP	**35**	6	3	14	3	2	7
	OFS	**6**	3	3	0	0	0	0
	OFAS	**15**	12	0	0	0	3	0
	OSAV	**14**	3	1	7	0	0	3
	MNS	**0**	0	0	0	0	0	0
	SWISS MEDIC	**31**	14	3	5	5	4	0
	SUVA	**7**	3	3	1	0	0	0
	Total	**126**	**52**	**15**	**31**	**8**	**9**	**11**
Département fédéral de justice et police DFJP	SG DFJP	**6**	5	0	1	0	0	0
	OFJ	**12**	8	0	4	0	0	0
	FEDPOL	**5**	2	0	3	0	0	0
	METAS	**4**	3	1	0	0	0	0
	SEM	**9**	3	3	0	1	1	1
	Service SCPT	**2**	0	2	0	0	0	0
	ISDC	**4**	2	0	1	1	0	0
	IPI	**0**	0	0	0	0	0	0
	CFMJ	**3**	3	0	0	0	0	0
	CAF	**0**	0	0	0	0	0	0
	ASR	**2**	0	2	0	0	0	0
	CSI	**1**	1	0	0	0	0	0
	CNPT	**0**	0	0	0	0	0	0
	Total	**48**	**27**	**8**	**9**	**2**	**1**	**1**

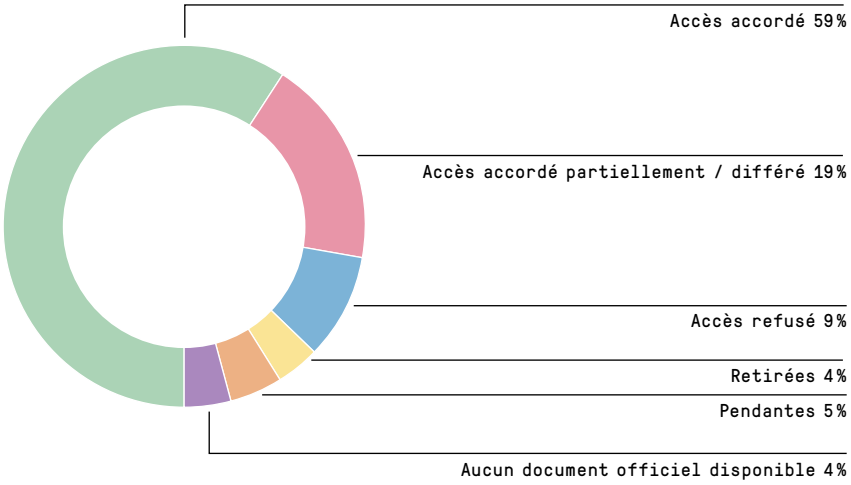
	Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	**5**	4	0	1	0	0	0
	Défens/armée	**24**	9	1	9	3	1	1
	SRC	**10**	1	3	3	1	1	1
	armasuisse	**7**	4	1	1	0	1	0
	OFSPO	**175**	172	1	0	1	1	0
	OFPP	**2**	2	0	0	0	0	0
	swisstopo	**2**	1	0	0	1	0	0
	OAC	**0**	0	0	0	0	0	0
	Total	**225**	**193**	**6**	**14**	**6**	**4**	**2**
Département fédéral des finances DFF	SG DFF	**16**	4	7	3	0	2	0
	UPIC	**4**	1	2	1	0	0	0
	AFF	**6**	4	0	2	0	0	0
	OFPER	**3**	3	0	0	0	0	0
	AFC	**14**	8	3	2	0	0	1
	ARD	**16**	5	3	6	2	0	0
	OFCL	**4**	4	0	0	0	0	0
	OFIT	**5**	5	0	0	0	0	0
	CDF	**10**	6	1	1	0	1	1
	SFI	**4**	2	1	1	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	DdC	**20**	7	0	9	0	1	3
	Total	**102**	**49**	**17**	**25**	**2**	**4**	**5**
Département fédéral de l'économie, de la formation et de la recherche DEFR	SG DEFR	**10**	4	1	4	0	1	0
	SECO	**34**	14	7	11	1	1	0
	SEFRI	**3**	2	0	0	0	0	1
	OFAG	**14**	5	2	2	1	3	1
	OFAE	**1**	0	0	1	0	0	0
	OFL	**0**	0	0	0	0	0	0
	SPR	**4**	1	1	1	0	1	0
	COMCO	**15**	12	0	3	0	0	0
	CIVI	**1**	1	0	0	0	0	0
	BFC	**2**	2	0	0	0	0	0
	FNS	**1**	0	0	1	0	0	0
	IFFP	**0**	0	0	0	0	0	0
	Conseil ETH	**9**	7	0	1	0	1	0
	Innosuisse	**6**	2	0	3	1	0	0
	Total	**100**	**50**	**11**	**27**	**3**	**7**	**2**

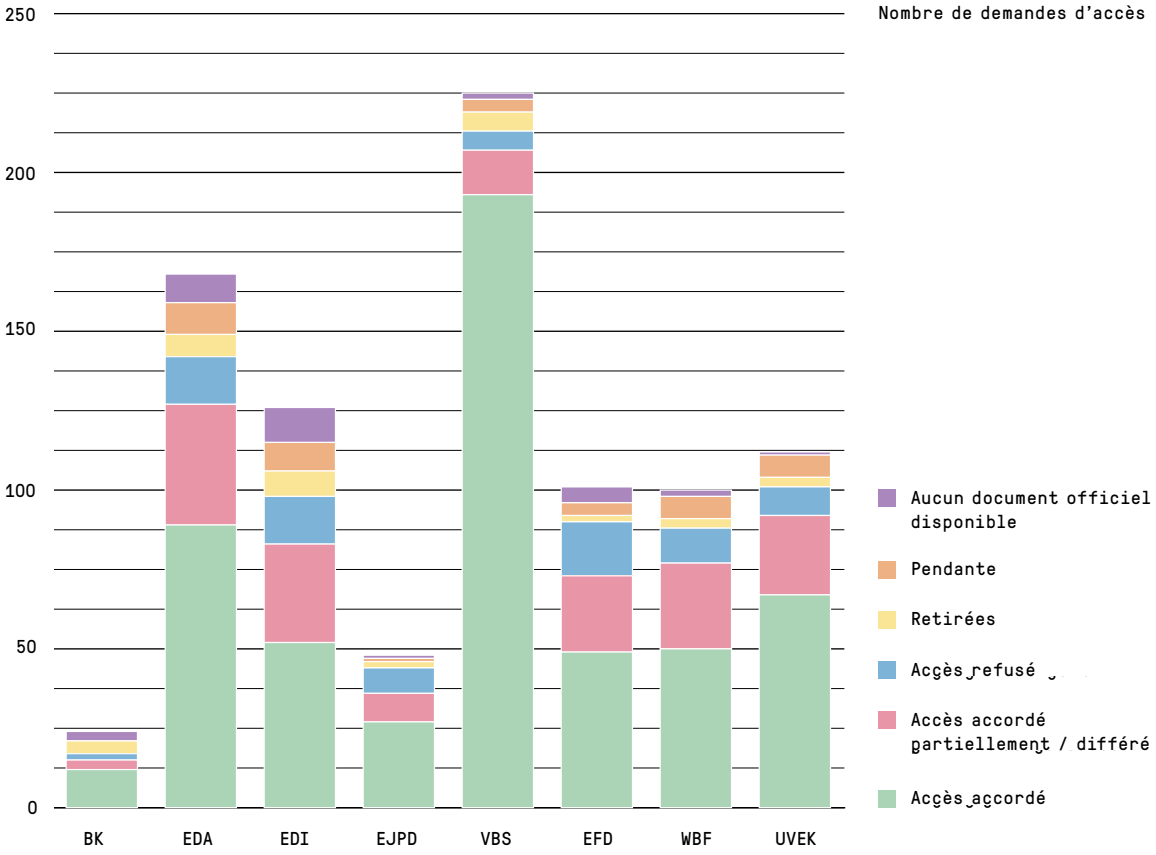
	Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	**10**	8	1	0	0	1	0
	OFT	**11**	8	0	3	0	0	0
	OFAC	**15**	7	2	2	0	3	1
	OFEN	**12**	6	0	4	1	1	0
	OFROU	**10**	9	0	0	0	1	0
	OFCOM	**4**	3	0	0	0	1	0
	OFEV	**35**	19	3	12	1	0	0
	ARE	**0**	0	0	0	0	0	0
	ComCom	**1**	1	0	0	0	0	0
	IFSN	**10**	3	2	4	1	0	0
	PostCom	**1**	1	0	0	0	0	0
	AIEP	**3**	2	1	0	0	0	0
	Total	**112**	**67**	**9**	**25**	**3**	**7**	**1**
Ministère public de la Confédération MPC	MPC	**10**	3	1	0	3	1	2
	Total	**10**	**3**	**1**	**0**	**3**	**1**	**2**
Services du Parlement SP	SP	**1**	0	1	0	0	0	0
	Total	**1**	**0**	**1**	**0**	**0**	**0**	**0**

Nombre de demandes en médiation

Catégories de requérants	2019
Médias	**34**
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	**40**
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	**7**
Avocats	**5**
Entreprises	**47**
Total	**133**

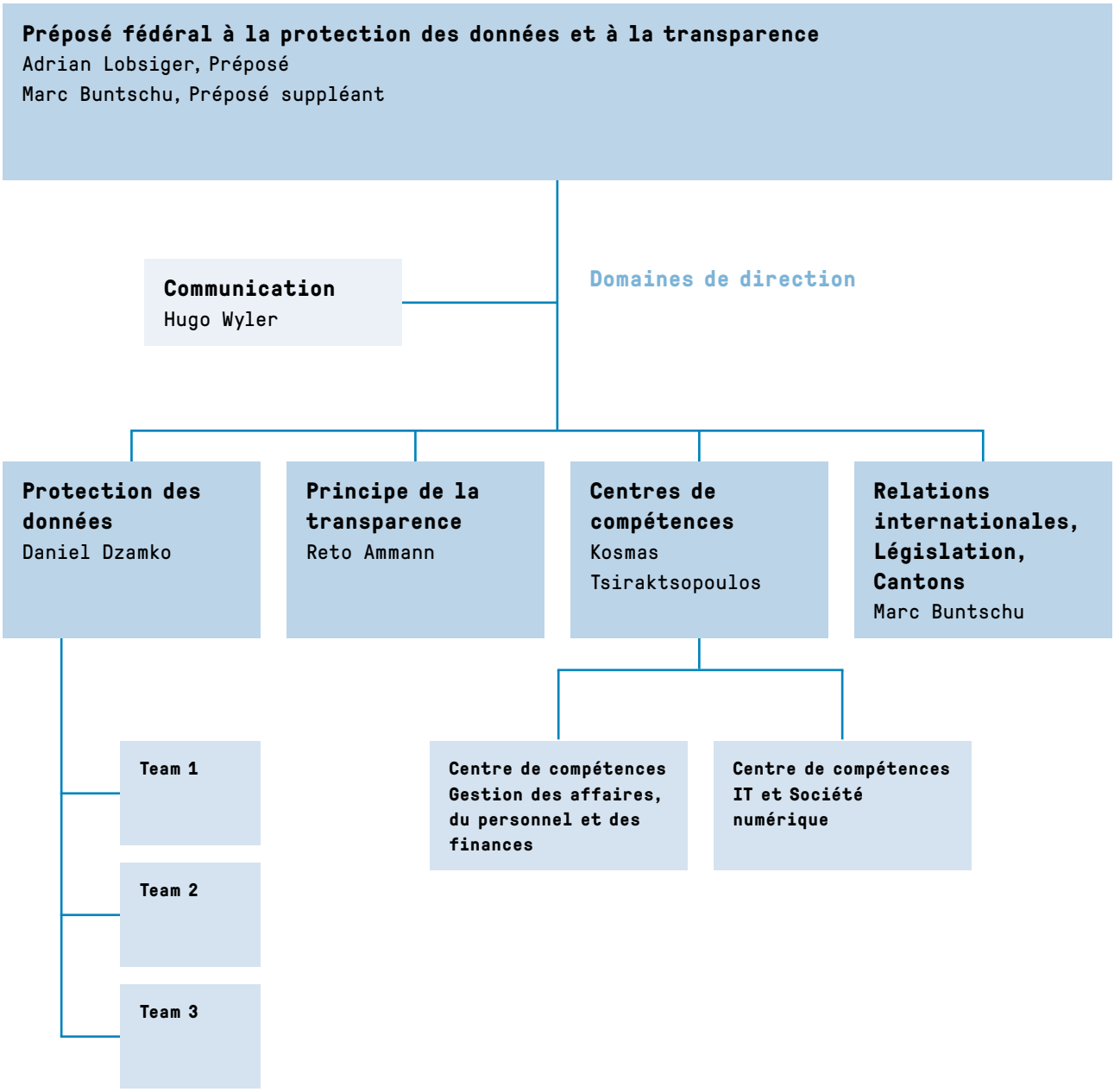
Traitment des demandes d'accès
du 1er janvier 2019 au 31 décembre 2019





3.4 Organisation du PFPDT (État 31 mars 2020)

Organigramme



Personnel du PFPDT

Nombre d'employés	37		
FTE	30.8		
par sexe	Femmes	19	51%
	Hommes	18	49%
par niveau d'emploi	1–89%	25	68%
	90–100%	12	32%
par langue	Allemend	29	78%
	Français	7	19%
	Italien	1	3%
par âge	20–49 ans	22	59%
	50–65 ans	15	41%
Postes dirigeants	Femmes	3	33%
	Hommes	6	67%

Liste des abréviations

ADR Alternative Dispute Resolution body (Organes indépendants de règlement extrajudiciaire des litiges dans le cadre du Privacy Shield)

AFAPDP Association francophone des autorités de protection des données

CEPD Comité européen de la protection des données

CIP Commission des institutions politiques (commission consultative chargée de la révision de la LPD)

CJUE Cour de justice de l'Union européenne

CNIL Commission Nationale de l'Informatique et des Libertés

Convention 108+ Convention 108 du Conseil de l'Europe pour la protection des données à caractère personnel modernisée

DEP Dossier électronique du patient

DoC Department of Commerce (Département du commerce des États-Unis)

EAR Échange automatique de renseignements relatif aux comptes financiers

EDPP Échange de déclarations pays par pays des grands groupes multinationaux

EIDCOM Commission fédérale des e-ID

Eurodac Base de données biométriques dans le domaine de l'asile de l'UE

fedpol Office fédéral de la police

FTC Federal Trade Commission (Autorité américaine de protection des consommateurs)

ICO Information Commissioner's Office (Autorité de protection des données du Royaume-Uni)

LPD Loi fédérale sur la protection des données

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

LTrans Loi fédérale sur le principe de la transparence dans l'administration

OCDE Organisation de coopération et de développement économiques

OFROU Office fédéral des routes

PCLOB Privacy and Civil Liberties Oversight Board (Organe indépendant de contrôle de la protection de la sphère privée et des libertés individuelles)

PNR Passenger Name Record (Données de passagers aériens)

Privatim Conférence des préposés suisses à la protection des données (autorités cantonales)

RIPOL Système de recherches informatisées de police

LPDS Loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal [SR 235.3]

RGPD Règlement européen de protection des données

Seco Secrétariat d'Etat à l'économie

SEFRI Secrétariat d'État à la formation, à la recherche et à l'innovation

SEM Secrétariat d'Etat aux migrations

SFI Secrétariat d'Etat aux questions financières internationales

SIRENE Supplementary Information Request at the National Entry (Point de contact national pour l'échange d'informations supplémentaires)

SIS Système d'information Schengen

SIS II Système d'information Schengen de la 2e génération

SYMIC Système d'information central sur la migration

T-PD Comité consultatif de la Convention 108

VIS Système d'information sur les visas

Table des illustrations

Graphiques

Tableaux

Les images apparaissant dans ce rapport se présentent comme une série de photos indépendantes du contenu et illustrent notre mobilité quotidienne, qui soulève de nombreuses questions en matière de protection des données. Certaines images ont été en partie pixélisées pour attirer l'attention sur le problème de l'identification et en même temps pour rendre les personnes et les entreprises non identifiables. Les photos ont été prises par le photographe biennois Ben Zurbriggen.

Chiffres clés

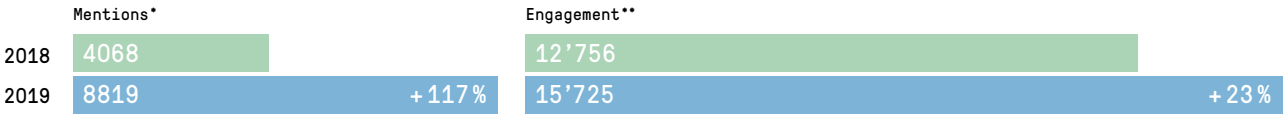
Dépenses de protection des données

49,8 %	16,7 %	24,2 %	9,3 %
Conseils	Surveillance	Information	Législation

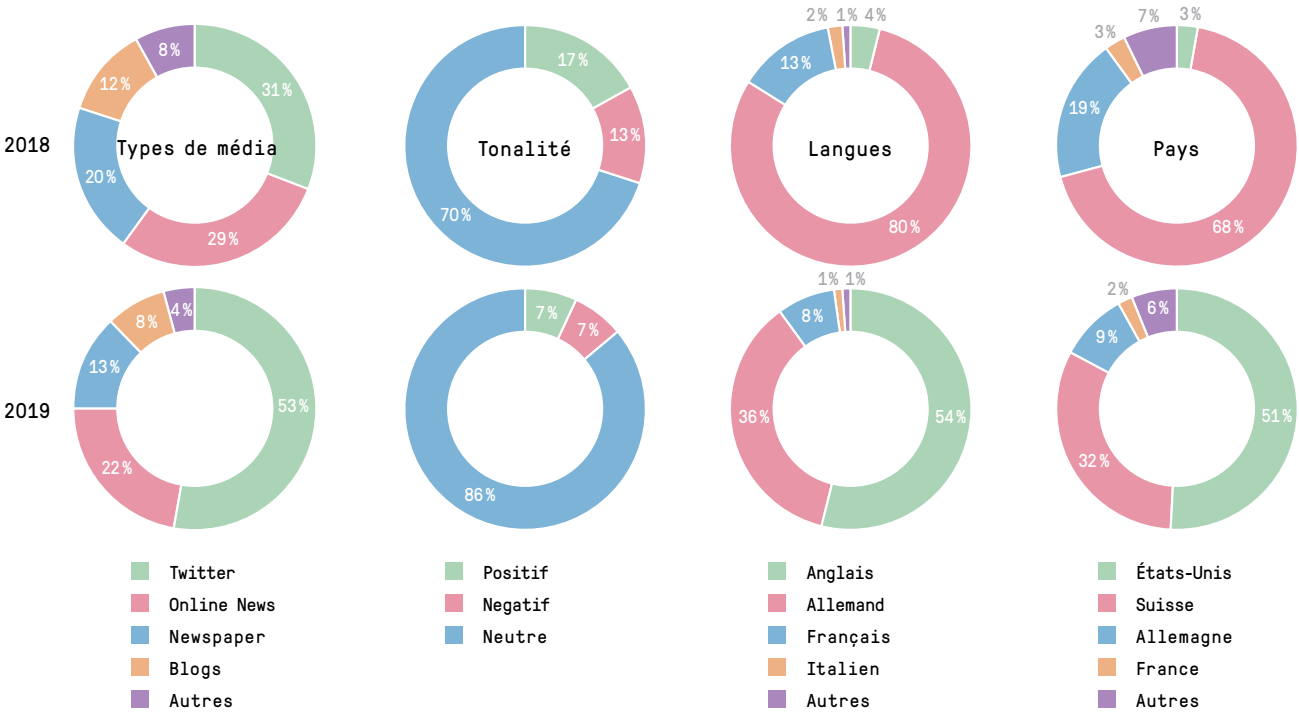
Demandes d'accès Principe de la transparence (LTrans)

59 %	19 %	9 %	4 %	5 %	4 %
accordé	accordé partiellement/ differé	refusé	retirées	pendantes	aucun document officiel disponible

Résonance médiale du Préposé sur le web social



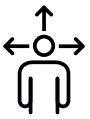
* Nombre de toutes les mentions du PFPDT (mentions dans Blogs, Twitter, Onlinenews, etc.)
** Nombre de toutes les interactions des contributions examinées (Likes, Retweets, etc.)



Préoccupations relatives à la protection des données

Transparence de l'information

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



Possibilité de choisir

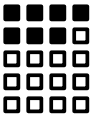
Les personnes concernées donnent leur consentement et jouissent d'une réelle liberté de choix.

Analyse des risques

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

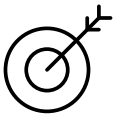
Exactitude des données

Le traitement s'effectue avec des données correctes.



Proportionnalité

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



Finalité

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

Sécurité des données

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

Documentation

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

Responsabilité individuelle

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

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. 410.027.F

Mise en page: Duplex Design GmbH, Basel
Photographie: Ben Zurbriggen
Caractères: Pressura, Documenta
Impression: Ast & Fischer AG, Wabern
Papier: PlanoArt®, holzfrei hochweiss

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

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