



25° Rapport d'activités 2017/18
Préposé fédéral à la protection
des données et à la transparence



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2017/2018

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 1^{er} avril 2017 au 31 mars 2018.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Avant-propos

Défis actuels et priorités

I	Digitalisation	6
II	Activité de conseil et de contrôle	7
III	Coopération nationale et internationale	8
IV	Mesures visant un accroissement de l'efficacité	9

1 Protection des données

1.1 Droits fondamentaux et questions d'ordre général 12

1.1.1	Révision de la loi fédérale sur la protection des données	12
1.1.2	Utilisation du numéro AVS comme identifiant personnel et évaluation des risques	13
1.1.3	Utilisation d'outils de gestion de campagne en ligne	14

1.2 Transports 15

1.2.1	Projets dans les transports publics	15
1.2.2	Traitement de données sur les véhicules	15
1.2.3	Circulation routière: introduction du tachygraphe intelligent	16

1.3 Internet et télécommunications 17

1.3.1	Téléviseurs intelligents (Smart TV)	17
1.3.2	Vol de données chez Swisscom	17
1.3.3	Mise en place d'une preuve d'identité électronique (e-ID)	17
1.3.4	Arrêt du Tribunal fédéral concernant le droit d'accès aux données secondaires	18

1.4 Justice, Police, Sécurité 19

1.4.1	Surveillance de la correspondance par poste et télécommunication: révision des dispositions d'application	19
1.4.2	Reconnaissance faciale à l'aéroport	20
1.4.3	Loi fédérale sur les précurseurs de substances explosibles et loi fédérale sur les mesures policières de lutte contre le terrorisme	20
1.4.4	Groupe de travail sur la révision de la loi sur les profils d'ADN	21
1.4.5	Collaboration dans l'espace Schengen	21
1.4.6	Contrôle des visas Schengen au SEM	22
1.4.7	Mise en œuvre Schengen: contrôle des signalements prononcés auprès du SEM	23

1.5 Santé et recherche 24

1.5.1	Dossier électronique du patient	24
1.5.2	Projet statistique BAGSAN	24
1.5.3	Davantage de transparence pour les patients en cas d'externalisation du traitement des factures de médecins	24
1.5.4	TARPSY, nouvelle structure tarifaire unique: extension des attributions des services de réception des données	25
1.5.5	La SUVA transmet des données sur les assurés à des fins de recherche	25

1.6 Assurances 26

1.6.1	Procurations dans le domaine des assurances d'indemnités journalières de maladie	26
1.6.2	Système d'information pour la lutte contre la fraude à l'assurance	26
1.6.3	Externalisation de tâches des assurances-maladie à des prestataires de services externes à la branche	26
1.6.4	Applications de santé et programmes bonus des assurances-maladie	27

1.7 Secteur du travail 28

1.7.1	Gestion électronique du recrutement: conclusion de la procédure d'établissement des faits	28
1.7.2	Un départ réussi en cas de résiliation des rapports de travail	28
1.7.3	Géolocalisation de collaborateurs	29
1.7.4	Saisie du temps de travail à l'aide des empreintes digitales dans la restauration	29

1.8	Économie et commerce	30
1.8.1	Privacy Shield entre la Suisse et les États-Unis	30
1.8.2	Fuite de données chez EOS Suisse	30
1.8.3	Révision de la loi sur le droit d'auteur	30
1.8.4	Publicité personnalisée dans les applications utilisant des données de localisation	31
1.8.5	Traitement de données chez Admeira	31
1.8.6	Lettre d'information concernant la carte client de Coop	31
1.8.7	Droits d'accès et d'opposition auprès d'un commerçant d'adresses – Résultat de la procédure devant le Tribunal administratif fédéral	32
1.8.8	Communication de données à des tiers par le site d'enchères ricardo.ch	32
1.8.9	Les questions admissibles dans les formulaires de demande de location	32
1.8.10	Ordonnances pour la mise en œuvre du premier train de mesures de la Stratégie énergétique 2050	33
1.8.11	Arrêt Moneyhouse	34
1.8.12	Centrale d'information de crédit	34
1.9	Finances	35
1.9.1	Échange automatique de renseignements	35
1.9.2	Établissement des faits auprès de l'Administration fédérale des contributions	36
1.10	International	37
2	Principe de la transparence	
2.1	Demandes d'accès	42
2.1.1	Départements et offices fédéraux	43
2.1.2	Services parlementaires	44
2.1.3	Ministère public de la Confédération	44
2.2	Demandes en médiation	45
2.3	Procédure de médiation: évaluation de l'essai pilote mené en 2017	46
2.3.1	Essai pilote	46
2.3.2	Respect du délai d'ordre	46
2.3.3	Proportion des solutions amiables	47
2.3.4	Analyse des questionnaires de retour d'expérience	47
2.3.5	Réduction du nombre de cas pendants	48
2.3.6	Résumé	48
2.4	Consultations des offices	49
2.4.1	Ordonnance sur le service de renseignement	49
2.4.2	Arrêt du Tribunal fédéral: accès aux déclarations d'atteintes à la sécurité et d'incidents dans les transports publics	49
2.4.3	Avant-projet d'ordonnance modifiant l'ordonnance sur l'accès aux documents du canton de Fribourg	50
3	Le PFPDT	
3.1	Tâches et ressources	52
3.2	Publications au cours de l'année sous revue	55
3.3	Statistiques	56
3.3.1	Statistiques des activités du PFPDT du 1 ^{er} avril 2017 au 31 mars 2018 (Protection des données et Principe de la transparence)	56
3.3.2	Statistique des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier 2017 au 31 décembre 2017	58
3.4	Le Secrétariat du PFPDT	64
	Liste des abréviations	66



Avant-propos

Face au rythme effréné de l'évolution numérique, notre autorité a de nouveau choisi de placer son activité sous le signe du pragmatisme au cours de l'exercice sous revue, ceci afin d'assurer une surveillance efficace.

Dans le cadre de la mise en œuvre de la loi sur la transparence, le recours à des procédures sommaires et principalement orales nous a permis de réduire considérablement la durée des procédures et de régler toutes les affaires en suspens, faisant grimper à 60 pour cent la proportion de solutions consensuelles. Ce pourcentage élevé d'accords est à nos yeux un signe supplémentaire de la consolidation progressive du changement de culture recherché par le législateur vers une activité administrative plus transparente.

Afin de s'assurer que les données personnelles soient traitées dans toute la mesure que la loi et non pas la technique permet, nous avons demandé aux responsables des applications numériques de documenter et réduire très tôt les risques en matière de protection des données. Ainsi, grâce à cette méthode de travail moderne, concrétisée par le projet de révision totale de la loi sur la protection des données qui s'appuie sur le nouveau droit européen, nous avons donc pu réduire notre propre charge de travail également dans le domaine de la surveillance de la protection des données.

Malgré cette efficacité accrue, la part de nos dépenses pour le conseil et le suivi de grands chantiers numériques a atteint pour la première fois un niveau record de plus de 50 pour cent au cours de l'exercice sous revue. Nos ressources étant restées pratiquement inchangées depuis 2005, cette évolution nous a contraints à faire preuve de retenue quant à l'ouverture de nouvelles procédures, de sorte que la proportion des clarifications de faits, déjà nettement inférieure au taux moyen de 20 pour cent au cours de la dernière période sous revue, est maintenant tombée à 12 pour cent. Nous avons ainsi effectué onze contrôles approfondis dans l'administration fédérale et dans des entreprises privées, ce qui témoigne d'une faible densité de contrôles compte tenu des quelque 12'000 moyennes et grandes entreprises qu'il y a en Suisse.

En dépit de tous ces enjeux, l'équipe du PFPDT mettra tout en œuvre, en sa qualité d'autorité de surveillance, pendant la délicate période de transition qui nous sépare de l'entrée en vigueur de la nouvelle loi sur la protection des données pour déployer une présence perceptible en Suisse et à l'étranger et apporter aide et conseil aux entreprises suisses dans l'application du nouveau règlement européen sur la protection des données, entré en vigueur en mai 2018.

Adrian Lobsiger

Préposé fédéral à la protection des données et à la transparence

Défis actuels et priorités

I Digitalisation

Les progrès des technologies de l'information et des télécommunications ainsi que le réseau mondial de l'économie ont créé une réalité numérique imprégnant au quotidien la vie des personnes vivant en Suisse, qu'il s'agisse de travail, de consommation ou de loisirs.

Technologie et économie

Outre les ordinateurs et les smartphones, de plus en plus de capteurs sont utilisés pour enregistrer nos photos, nos voix et même des fonctions corporelles internes et, grâce à l'élargissement de la bande passante, de l'Internet des objets, pour alimenter des intelligences artificielles dont l'objectif est de répondre à un maximum de besoins et intérêts commerciaux, scientifiques, politiques ou autres, avec un minimum de ressources.

La protection des données exige que l'évaluation, l'analyse et la prévision des besoins soient toujours basées sur des technologies informant de manière conviviale et complète les utilisateurs, qu'ils soient clients, consommateurs, passagers ou patients, sur les objectifs et les modes de fonctionnement des applications utilisées. Un autre point essentiel est l'investissement dans des technologies offrant une protection efficace contre l'accès non autorisé aux données personnelles. Au cours de l'exercice sous revue, le PFPDT a traité un grand nombre de cas de pertes de données, ce qui montre bien que la sécurité technique ne progresse pas au même rythme que la collecte, la diffusion et l'exploitation des données. Comme après les catastrophes qui ont marqué la commercialisation des moteurs à réaction dans l'aéronautique des années 60, la technologie de la sécurité doit rattraper ce retard. Cela n'est possible que si les responsables des traitements de données anticipent les risques et réalisent les investissements nécessaires dans ce but.

Société, politique et droit

La réalité numérique est façonnée par des acteurs qui usent de leur savoir-faire technique pour exploiter commercialement, scientifiquement ou politiquement les données d'autrui et dont les offres générées de manière automatique ciblent majoritairement des utilisateurs non experts. Le respect du droit à l'autodétermination informationnelle exige que même ceux dont l'accès au savoir-faire technique est limité puissent participer judicieusement à la numérisation. C'est dans cet objectif que la protection des données établit, au niveau des autorités et des entreprises, des passerelles permettant la circulation du savoir entre les fournisseurs de services numériques et les utilisateurs. Malheureusement, la nécessité d'une

information adaptée et complète n'est pas reconnue par tous les responsables. Lorsque les clients apprennent par des lanceurs d'alerte l'utilisation de leurs données, comme dans le cas de Cambridge Analytica, la confiance entre utilisateurs et fournisseurs de services numériques s'étioule, ce qui, comme pour Facebook, appelle les régulateurs et les autorités de surveillance à intervenir.

Les données de navigation présentent un risque particulier d'atteinte à la sphère privée. En effet, à partir des sites consultés, il est possible de tirer des conclusions sur les motivations des utilisateurs à cibler tel contenu sur Internet. Sur la base de très brèves périodes d'accès à Internet, ces données génèrent des profils de la personnalité suggérant des intérêts, des préférences ou des contacts et donc indirectement des schémas de pensée et d'attitude, jusqu'à l'orientation sexuelle et les fantasmes intimes. Bien que techniquement réalisable, le traitement des profils de navigation ne doit jamais permettre d'extraire le comportement de personnes identifiables – hormis dans le cas des ordonnances pénales. Jusqu'à présent, le PFPDT n'avait pas les moyens de vérifier, si ce n'était sur la base de contrôles techniques élaborés, dans quelle mesure les responsables des applications qui postent des messages à l'intention de groupes d'utilisateurs, respectent effectivement l'interdiction d'identifier des personnes. En outre, le débat public sur l'affaire Cambridge Analytica et Facebook montre que les plates-formes sociales dont les utilisateurs disposent d'un compte soulèvent des questions délicates de délimitation. Dans la période sous revue, dans le contexte de ce que l'on nomme le micro-ciblage, notre autorité concentre ses efforts pour que les auteurs des applications en question et leurs finalités commerciales, politiques ou autres soient totalement transparents avant qu'un consentement ne soit demandé à l'utilisateur. Dans la perspective des prochaines élections fédérales, le PFPDT s'est adressé à l'automne 2017 aux organisateurs des campagnes politiques en publiant un feuillet thématique abordant aussi ce sujet (www.leprepose.ch, Protection des données – Documentation – Feuilles thématiques – Utilisation d'outils numériques de gestion de campagne à des fins politiques).

Afin de pouvoir s'assurer, en tant qu'autorité de contrôle, que le traitement de données à caractère personnel ne soit pas aussi poussé que la technique le permet, mais demeure dans le cadre légalement admissible, le PFPDT demande aux responsables des applications numériques de réduire déjà en amont les risques élevés touchant à la protection des données et de les signaler aux conseillers à la protection des données des entreprises et aux autorités de contrôle compétentes. Le numérique offre aujourd'hui des procédés de travail modernes tels que l'évaluation des risques en matière de protection des données. Ces procédés ont également été appliqués dans des grands projets que le PFPDT a accompagnés (voir ch. 3.1 du présent rapport) bien avant l'entrée en vigueur du nouveau Règlement général de l'UE sur la protection des données (RGPD). Il en va de même de la notification de violations de données: uniquement pendant le mois de décembre 2017, trois entreprises ont signalé des faits graves au PFPDT.

Il est donc d'autant plus étonnant que l'examen de la révision totale de la loi sur la protection des données de 1993, présentée par le Conseil fédéral le 15 septembre 2017 dans le but de mettre en place et de concrétiser ces instruments de travail, ait été retardé par la Commission des institutions politiques du Conseil national en qualité de premier conseil. À la suite de la décision de la Commission de limiter ces innovations au traitement des données par les autorités de poursuite pénale dans le cadre d'une mise en œuvre anticipée de la «directive Schengen», la révision totale a dû être reportée et les discussions suspendues jusqu'à ce que l'administration ait élaboré un projet législatif à ce sujet. Cela a une conséquence: la protection des données de la population suisse repose toujours sur une loi vieille de 25 ans, entrée en vigueur douze ans avant la commercialisation du premier smartphone et ne reflétant en rien la réalité numérique.

II Activité de conseil et de contrôle

Au cours l'exercice 2017–2018, nous avons poursuivi l'accompagnement consultatif de plusieurs grands projets big data des autorités fédérales et du secteur privé. À cette occasion, nous nous sommes penchés sur le risque de ré-identification inappropriée de personnes à partir de données factuelles. En outre, eu égard aux pertes de données dont il a été question plus haut et dans le cadre de leurs accompagnements de projet, les équipes interdisciplinaires du PFPDT ont eu toujours plus fréquemment à examiner les mesures techniques et organisationnelles pour réduire les risques de perte.

Bien que le PFPDT insiste pour que nous utilisions les outils de la technologie moderne déjà mentionnés afin d'évaluer les risques élevés en matière de sécurité, réduisant ainsi notre charge de travail, la part de nos charges totales en matière de conseil pour les projets du secteur privé a atteint un nouveau niveau record au cours de l'exercice sous revue (voir ch. 3.1 du présent rapport). Outre la complexité croissante des projets big data, cette augmentation s'explique par les déclarations de pertes de données, à la suite desquelles les entreprises concernées se sont adressées à nous pour des prestations de conseil. Le PFPDT a donc dû dégager à court terme des ressources humaines considérables car la réduction des dommages et l'information des clients ne souffrent aucun retard. Compte tenu des moyens limités dont nous disposons, cette situation a entraîné des retards et des suppressions dans les contrôles planifiés. Toujours en ce qui concerne le traitement des données personnelles par les applications grand public et les réseaux sociaux, le Préposé est arrivé au bout de ses ressources déjà limitées de sorte qu'il n'a pas été en mesure, à cet égard, de répondre aux attentes du public avec la proactivité souhaitée.

III Coopération nationale et internationale

Le PFPDT a intensifié sa coopération avec les autorités cantonales et communales de protection des données, qui sont confrontées aux mêmes développements et technologies quant au traitement des données personnelles. Depuis le 25 octobre 2017, il est membre associé, c'est-à-dire sans droit de vote, de l'association Privatim, au sein de laquelle il détient néanmoins une voix consultative. À propos de la révision totale de la loi sur la protection des données, Privatim a exprimé une position publique partiellement différente de celle du PFPDT.

Nouveau règlement européen sur la protection des données

Le nouveau Règlement européen sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018. Dans certaines conditions, il sera également applicable aux traitements de données par les entreprises suisses. À l'automne 2017, le PFPDT a publié un feuillet thématique qui aborde en particulier l'application extraterritoriale du nouveau droit européen (www.leprepose.ch, RGPD). Il a également participé à de nombreuses séances d'information sur ce sujet et a répondu à de nombreuses questions orales et écrites des citoyens et des médias dans le cadre de son activité de conseil.

La période de transition nous séparant de la nouvelle loi sur la protection des données (LPD), dont l'entrée en vigueur est désormais retardée (voir ch. 1.1.1 et 3.1 du présent rapport), sera un défi particulier pour notre autorité. Alors que les entités chargées de la protection des données dans les États membres de l'UE sont désormais dotées de pouvoirs de décision et de sanction et bénéficient de ressources supplémentaires considérables, le PFPDT n'a, jusqu'à nouvel ordre, que les pouvoirs de recommandation prévus par la LPD de 1993 et les mêmes moyens qu'en 2005 (voir ch. 3.1 du présent rapport). Il continuera néanmoins à tout mettre en œuvre pour conseiller et soutenir les entreprises suisses concernées dans l'application du RGPD et, en tant qu'autorité de surveillance, à développer une présence également perceptible à l'étranger. Ce dernier point est important dans la mesure où les autorités de surveillance des États membres de l'UE possèdent de nouveaux mécanismes renforcés pour regrouper leurs activités de surveillance, y compris en ce qui concerne le traitement des données dans les pays tiers. Il convient également de noter que les institutions de l'UE évaluent régulièrement dans quelle mesure les pays tiers, comme la Suisse, disposent d'une protection des données comparable à celle de l'UE.

Le groupe de travail «article 29» sur la protection des données a été remplacé par le «Comité européen de la protection des données» lorsque le RGPD est entré en vigueur. Au cours du premier semestre 2018, le PFPDT a pris contact avec le Comité et a demandé le statut d'observateur. Le rôle principal du Comité sera d'assurer l'application uniforme du Règlement général.

Swiss-US Privacy Shield

Au cours de l'année sous revue, nous avons participé en tant qu'observateurs à la première évaluation du Privacy Shield UE-États-Unis. À l'automne 2018, nous procéderons à la première évaluation du Privacy Shield Suisse-États-Unis; cette évaluation suivra à Bruxelles la deuxième évaluation du Privacy Shield UE-États-Unis. Cette évaluation se fera en étroite coordination temporelle et matérielle avec l'UE (voir ch. 1.8 du présent rapport).

IV Mesures visant un accroissement de l'efficacité

Face à ces défis, le Préposé réaffirme son objectif stratégique d'accomplir, dans un monde devenu numérique, ses tâches légales d'une manière compétente, indépendante et proactive.

Organisation et contrôle des affaires de l'autorité

La réorganisation de notre autorité, entrée en vigueur le 1^{er} avril 2017, s'est avérée positive et se consolide. L'interaction des collaborateurs au sein d'équipes interdisciplinaires et leur développement professionnel méritent une attention particulière. En raison de la charge de travail élevée, ce dernier point ne peut être atteint dans la mesure où le progrès technique induit par la numérisation le nécessiterait.

Le PFPDT accomplit de manière autonome ses tâches légales en tant qu'autorité de surveillance. Il bénéficie toutefois du soutien logistique et administratif de l'administration fédérale qui fournit ces prestations conformément aux normes générales de l'administration fédérale. En ce sens, le PFPDT est également assisté par la Chancellerie fédérale dans l'introduction du nouveau système de gestion des affaires Acta Nova.

Au cours de la période sous revue, le PFPDT a également mis en place «Cockpit», un instrument permettant de hiérarchiser et de gérer les activités de surveillance de la protection des données, qui sera également exploité à l'avenir par l'intermédiaire d'Acta Nova.

Offre d'information

L'offre d'informations et le Rapport d'activités ont déjà fait l'objet d'un remaniement au cours de la période sous revue, mais doivent être encore améliorés. Compte tenu de la forte charge d'affaires, ces ajustements ont pris du retard.

Procédure dans le domaine de la loi sur la transparence (LTrans)

A titre d'essai pendant un an, le PFPDT a introduit en date du 1^{er} janvier 2017 une procédure sommaire et accélérée généralisant les procédures de médiation orales. Cette expérience s'étant révélée positive et l'objectif de traiter tous les cas en suspens ayant été atteint, cette nouvelle méthode de travail a désormais été adoptée de manière permanente.



Protection des données

1.1 Droits fondamentaux et questions d'ordre général

1.1.1 Révision de la loi fédérale sur la protection des données

Le 15 septembre 2017, le Conseil fédéral a adopté le message à l'intention du Parlement concernant la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres actes législatifs. L'objectif de cette révision tend en particulier à renforcer la protection des données, notamment par une amélioration de la transparence des traitements et un meilleur contrôle par les personnes sur les données qui les concernent.

La révision doit permettre à notre législation de répondre au défi de la numérisation de la société, reprendre la «Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil» (acquis de Schengen), se rapprocher des exigences du «Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE» (Règlement général sur la protection des données) et ratifier la Convention 108 modernisée. Elle doit aussi contribuer à maintenir la reconnaissance par l'Union européenne du niveau de protection adéquat de notre pays.

Comme nous l'avons communiqué le même jour que la publication du Message (FF 2017 6565) concernant la révision totale de la loi fédérale sur la protection des données (cf. notre appréciation publié sur le site), nous approuvons les grandes lignes de la révision.

Nous nous félicitons notamment de l'amélioration de la transparence en matière de traitement des données; le devoir d'information lors de la collecte est en effet étendu à tous les traitements dans le secteur privé, indépendamment de la nature des données. Nous saluons également l'introduction d'une obligation de procéder à une analyse d'impact relative à la protection des données pour les projets qui présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. L'extension de l'obligation d'informer les personnes concernées sur leurs droits d'accès est également un point positif. Il en va de même de l'encouragement de l'autoréglementation, par le biais de codes de conduite qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Nous

relevons également l'introduction explicite des principes de la protection des données dès la conception et par défaut (Privacy by design et Privacy by default). Notre indépendance et nos pouvoirs sont en outre renforcés. Le projet de loi prévoit que nous pourrions prendre, à l'instar de nos homologues européens, des décisions contraignantes à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur dénonciation. Nous prenons avec satisfaction acte du fait que le Conseil fédéral prévoit de nous allouer des moyens supplémentaires indispensables à l'exécution de la nouvelle loi.

Tout en approuvant les grandes lignes de la révision, nous avons émis quelques réserves dues notamment au fait que le projet du Conseil fédéral présente des différences terminologiques et matérielles par rapport au règlement général de l'UE sur la protection des données et à la convention 108 modernisée. Nous estimons que nombre de ces différences ne sont pas judicieuses, notamment parce qu'elles compliquent inutilement la situation juridique des entreprises suisses et des services de l'administration qui seront directement soumis au règlement général de l'UE sur la protection des données et qu'elles créent une insécurité juridique.

En outre, nous avons vainement plaidé pour une adoption rapide du projet. La Commission des institutions politiques du Conseil national (CIP-CN) a décidé de scinder la révision en deux et d'élaborer, dans un premier temps, une loi sur la protection des données limitée, dans son champ d'application, aux autorités fédérales de poursuite pénale afin de tenir compte des modifications en lien avec l'acquis de Schengen; ce qui a eu lieu en avril 2018. En raison de ce choix, le Conseil national débattrait, lors de sa session d'été, de ce projet de loi Schengen au lieu de la révision totale de la loi.

Nous aurions néanmoins souhaité l'introduction d'un droit à la portabilité des données. Ce droit renforcerait le contrôle de l'utilisateur sur ses données personnelles. Nous préconisons l'introduction d'une obligation de démontrer la mise en conformité laquelle permettrait un renversement du fardeau de la preuve. Nous proposons également que la nouvelle loi, à l'instar du règlement général de l'UE sur la protection des données, s'applique expressément aussi aux entreprises n'ayant pas de siège en Suisse mais qui procèdent à des traitements ayant des effets en Suisse, afin que les personnes concernées puissent exercer plus facilement leurs droits. A cet effet, ces entreprises devraient avoir un interlocuteur en Suisse. Le nouveau droit suisse devrait soumettre la désignation des conseillers à la protection des données en entreprise aux mêmes conditions que celles que prévoit le règlement

général de l'UE sur la protection des données en ce qui concerne les entreprises directement soumises à celui-ci. Il en va de même pour les codes de conduite. Les associations professionnelles et les associations économiques suisses devraient nous les soumettre selon les mêmes règles que celles qu'elles doivent respecter en vertu du règlement général de l'UE. Il serait en outre nécessaire que les entreprises dotées d'un conseiller à la protection des données soient également soumises aux obligations en matière d'analyses d'impact. De même les traitements de données présentant un risque particulièrement élevé devraient faire l'objet d'une certification.

Les sanctions prévues (amende de 250'000 francs au plus) sont peu dissuasives au regard de celles fixées par le règlement général de l'UE sur la protection des données (20 millions d'euros ou 4 % du chiffre d'affaires annuel) ou de celles prévues dans la loi fédérale sur la concurrence qui a amené le Tribunal fédéral à condamner une firme automobile allemande à verser une amende de 150 millions de francs. Nous préconisons dès lors de revoir le système des sanctions. Enfin, notre budget ne devrait pas être approuvé par le Conseil fédéral mais par le Parlement, à l'instar du régime appliqué aux autres autorités de surveillance indépendantes telles que le Contrôle fédéral des finances et le Service de renseignement de la Confédération.

En avril 2018, la CIP-CN a adopté la nouvelle loi sur la protection des données Schengen qui sera soumise au Conseil national lors de la session d'été. Nous espérons dès lors que la révision totale de la loi sur la protection des données puisse désormais rapidement être abordée par le Parlement.

1.1.2 Utilisation du numéro AVS comme identifiant personnel et évaluation des risques

Le Conseil fédéral a chargé le Département fédéral de l'intérieur (DFI) d'élaborer un projet de loi afin de faciliter l'utilisation du numéro AVS par toutes les collectivités fédérales, cantonales et communales également en dehors du domaine de la sécurité sociale. Sur mandat confié par le PFPDT conjointement avec l'Office fédéral de la justice (OFJ) David Basin, professeur ordinaire à l'EPF de Zurich, a présenté fin septembre une analyse des risques en matière de protection des données concernant l'utilisation d'identifiants personnels et l'extension prévue du champ d'application du numéro AVS.

Afin d'améliorer l'efficacité des procédures administratives, le 1^{er} février 2017, le Conseil fédéral a chargé le Département fédéral de l'intérieur (DFI) d'élaborer un projet de loi dont l'objectif est de faciliter l'utilisation du numéro AVS par toutes les collectivités fédérales, cantonales et communales également en dehors du domaine de la sécurité sociale. Dans le cadre des travaux préparatoires de cette proposition, un groupe de travail interne à l'administration avait conclu, après examen, que l'utilisation du numéro AVS comme identifiant personnel ne présentait pas de risques particuliers. Le PFPDT n'était pas représenté dans ce groupe de travail, bien que les autorités fédérales et cantonales de protection des données se soient ces dernières années constamment prononcées en faveur d'identifiants sectoriels et contre l'extension du numéro AVS en dehors du domaine de la sécurité sociale.

Le Parlement a, à plusieurs reprises, dû se prononcer sur l'utilisation du numéro AVS comme identifiant personnel en dehors du domaine de la sécurité sociale, comme dans le dossier électronique du patient, le registre du commerce et l'échange automatique d'informations en matière fiscale. Ce fut également le cas dernièrement dans le cadre du projet de révision du registre foncier.

Afin d'approfondir davantage les risques spécifiques aux identificateurs, nous avons donné, conjointement à l'OFJ, un mandat externe en vue d'une évaluation des risques. Suite à une procédure d'invitation, l'évaluation a été adjugée au Professeur David Basin, professeur ordinaire de sécurité de l'information au Département de l'informatique à l'EPF de Zurich. L'expertise devait préciser en particulier si des risques – et, le cas échéant, lesquels – peuvent survenir selon le type d'identifiant utilisé et selon l'étendue de leur usage. Dans son évaluation de l'impact des risques du 27 septembre 2017, le professeur Basin précise l'ampleur des risques comme suit:

«Des données personnelles, souvent sensibles, sont conservées dans plus de 14 000 registres tenus par des services administratifs ou d'autres organismes et indexés au moyen d'un identifiant unique, le numéro AVS à 13 chiffres (NAVS13). Les données et les systèmes informatiques utilisés pour les conserver peuvent faire l'objet d'attaques tant internes qu'externes [...]. Ces risques pour la protection des données vont se renforcer au fur et à mesure de l'augmentation du nombre d'organismes ayant recours au NAVS13 pour le traitement de données et de l'accroissement du volume de données collectées, conservées et traitées, en particulier par des administrations cantonales et communales et des organismes privés utilisant des systèmes informatiques non fédéraux relativement peu sûrs.

Les données des registres étant conservées avec les attributs relatifs à l'identité qui leur sont associés, le seul remplacement du NAVS13 par des identifiants sectoriels ou d'autres pseudonymes ne réduirait guère les risques pour la protection des données [...] Il existe cependant des moyens de réduire considérablement ces risques. Ces moyens impliquent de repenser la manière dont les données sont conservées, traitées et sécurisées.

Les mesures suivantes permettraient de réduire nettement les risques qui pèsent aujourd'hui sur la protection des données, en particulier les risques consécutifs à l'expansion continue du mode actuel d'utilisation du NAVS13. L'une de ces mesures consiste à introduire des pseudonymes non significatifs (tels que le numéro de contribuable ou le numéro du dossier électronique du patient) en respectant certains principes et à éviter autant que possible de les conserver dans les registres avec d'autres attributs relatifs à l'identité. Cette mesure peut être mise en œuvre en utilisant des identifiants sectoriels, qui peuvent prendre différentes formes. [...]»

Après avoir pris connaissance de ce document, le 20 octobre 2017, la Commission des affaires juridiques du Conseil national a déposé un postulat chargeant le Conseil fédéral de montrer dans un concept, pendant la législature en cours, de quelle manière il est possible de faire face aux risques liés à l'utilisation du NAVS13 en tant qu'identifiant unique des personnes. Le concept devra en outre montrer de quelle manière la protection des données peut être améliorée dans le cadre de l'utilisation de numéros d'identification de personnes par les cantons, les communes et des tiers et prendra pour cela en considération l'avis du PFPDT. Le Conseil fédéral a accepté le postulat le 20 décembre 2017.

Il incombe désormais au Conseil fédéral et à son administration de tirer, au niveau fédéral, les conséquences qui s'imposent de cette analyse des risques approfondie. De même, nous attendons que l'Office fédéral des assurances sociales (OFAS) explique, en connaissance de l'évaluation de l'impact sur les risques, les conclusions à tirer de la soumission pour une utilisation générale du numéro AVS dans le cadre de son projet de révision de la loi fédérale sur l'assurance-vieillesse (LAVS).

Nous restons particulièrement attentifs à cette évolution et attendons de l'administration fédérale qu'elle formule, dans la perspective de l'utilisation d'identifiants personnels, des solutions qui répondent de manière adéquate à la fois aux préoccupations légitimes concernant l'efficacité de l'administration et aux exigences de protection et de sécurité des données. Une telle démarche apparaît assez urgente, au vu des projets numériques de grande ampleur en relation avec l'identification électronique qui soulèvent des problématiques similaires (cf. chiffre 1.3.3 du présent rapport).

Le rapport concernant l'évaluation des risques se trouve sur notre site à l'adresse suivante : www.leprepose.ch, Protection des données – Statistique, registre et recherche – Numéro AVS.

1.1.3 Utilisation d'outils de gestion de campagne en ligne

Les outils de gestion de campagne en ligne permettent à des groupements politiques et communautés d'intérêts d'organiser numériquement leurs contacts personnels et d'axer leurs campagnes sur des interactions ciblées. Ce mode d'action étant de plus en plus populaire, nous avons publié un feuillet thématique concernant la protection des données dans ce domaine.

Au cours de l'année sous revue, en réponse à des demandes de journalistes et de partis politiques, nous avons élaboré un document explicatif sur les aspects de protection des données en relation avec l'utilisation d'outils numériques de gestion de campagne. Ces outils sont des applications permettant à des groupements politiques et communautés d'intérêts d'intégrer certaines actions sur leurs pages Internet, afin d'axer la planification et l'exécution de leurs campagnes sur l'interaction ciblée avec certains groupes de personnes. Ces modes d'action reposent sur les données de personnes ayant manifesté leur intérêt, par exemple en s'enregistrant sur le site Internet d'un parti.

L'utilisation d'outils numériques de gestion de campagne doit se conformer à certains impératifs de protection des données, en particulier aux principes de transparence et de finalité. Nous avons d'abord souligné que les personnes concernées devaient recevoir une information claire et exhaustive sur le traitement des données avant leur enregistrement. Le traitement ne peut avoir lieu que si l'utilisateur, sur la base de cette information, a explicitement donné son consentement dans le cadre de son droit à l'autodétermination. Cela signifie également que les personnes concernées doivent avoir la possibilité de révoquer à tout moment leur consentement. En vertu du principe de finalité, les groupements politiques et communautés d'intérêts doivent limiter leurs traitements de données avec les outils en question aux finalités qui ont fait l'objet d'un consentement. Il convient également de souligner qu'un éventuel croisement des données personnelles avec des informations provenant d'autres sources, par exemple de plateformes de médias sociaux, présuppose un consentement séparé des personnes concernées.

Notre feuillet thématique a été publié sur le site www.leprepose.ch – Protection des données – Documentation – Feuilles thématiques.

1.2 Transports

1.2.1 Projets dans les transports publics

Au cours de l'année sous revue, le secteur des transports et plus particulièrement les CFF nous ont informés sur plusieurs projets ayant un impact en matière de protection des données. Il s'agit d'une part de l'utilisation des caméras corporelles (bodycams) et d'autre part du développement de nouvelles applications. Le délégué à la protection des données des CFF avait analysé au préalable l'impact de ces projets dans le domaine du droit de la protection des données.

Cette année encore, nous avons consacré une grande part de notre activité de conseil au secteur des transports. Au contraire de la procédure d'établissement des faits, l'accompagnement consultatif des projets se limite en règle générale à des évaluations sommaires, destinées à identifier précocement les problèmes en relation avec la protection des données (cf. également chiffre 1.2.3 du 24^e rapport d'activités 2016/2017). La direction des CFF nous a présenté différents projets, qui ont fait l'objet par la suite d'un accompagnement technique. Pour affecter le plus rationnellement possible nos ressources limitées, nous avons demandé que les projets et les problématiques qu'ils soulèvent en matière de protection des données nous soient présentés seulement après examen préliminaire par le service interne de protection des données des CFF.

Parmi les projets portés à notre attention, un essai pilote a été mené par les CFF pour tester l'utilisation de bodycams. Il s'agit d'appareils d'enregistrement vidéo et audio que les collaborateurs de la police des transports portent directement sur eux. Ce projet est encore en phase d'évaluation. Les CFF nous ont également informés de leur gestion des données de clients et du développement de diverses applications, en particulier l'application mobile SwissPass. Dans le cadre de notre accompagnement, nous avons souligné certains problèmes en relation avec la protection des données et partons du principe que nos recommandations seront suivies dans la suite des travaux sur ce projet. Nous continuerons d'accompagner le secteur des transports, et veillerons notamment à ce que toutes les personnes qui le souhaitent aient la possibilité de voyager de façon anonyme sans contrepartie financière sous forme de suppléments tarifaires.

1.2.2 Traitement de données sur les véhicules

La numérisation croissante entraîne d'importants traitements de données collectées dans les véhicules. Nous avons conseillé un constructeur automobile, qui va mettre en œuvre nos recommandations.

Le développement du numérique offre un potentiel énorme au secteur automobile. Des quantités croissantes de données sont collectées dans des véhicules, pour être couplées et transmises à des tiers. Diverses autorités de protection des données ont donc récemment élaboré des procédures de bonnes pratiques (best practices), par exemple la Conférence des autorités indépendantes de protection des données d'Allemagne et l'Association allemande de l'industrie automobile.

Au cours de l'année sous revue, nous avons examiné le traitement des données sur les véhicules par un constructeur automobile. Nous avons mis l'accent sur la transparence de l'information au détenteur du véhicule, les transmissions de données à l'étranger et les déclarations de consentement univoques. Le constructeur automobile a pris connaissance de nos remarques et les a mises en œuvre.

1.2.3 Circulation routière: introduction du tachygraphe intelligent

Nous avons pris position sur les bases légales devant encadrer l'introduction d'un tachygraphe intelligent. Nous avons critiqué l'insuffisance de l'information sur l'accès aux données et l'absence de prescription concernant la durée de conservation des données collectées par les services de police.

Dans le cadre de la consultation des offices, notre prise de position en matière de protection des données a été sollicitée concernant l'introduction d'un nouveau type de tachygraphe. Ce projet implique l'adaptation du droit suisse aux prescriptions européennes dans diverses ordonnances. Le tachygraphe intelligent simplifie considérablement la collecte de données. Il est relié à un système de satellite mondial et saisit notamment la localisation précise du véhicule. Différentes entités, notamment l'employeur du conducteur ou les services de police, peuvent accéder à ces données. Dans notre prise de position, nous avons souligné que les conducteurs des véhicules devaient être mieux informés de cet accès aux données par des tiers, afin de garantir le respect du principe de transparence. Nous avons également déploré l'absence de réglementation concernant la durée de conservation des données collectées par la police par le biais du tachygraphe. Le règlement correspondant de l'UE prévoit une durée d'archivage de trois heures dans les cas où le véhicule n'est pas contrôlé et à moins qu'une manipulation ou qu'une utilisation abusive du tachygraphe ne soient constatées. Nous avons demandé l'intégration de prescriptions analogues dans l'ordonnance sur le contrôle de la circulation routière.

1.3 Internet et télécommunications

1.3.1 Téléviseurs intelligents (Smart TV)

Nous avons ouvert une procédure auprès d'un fabricant de téléviseurs intelligents afin de contrôler la conformité des traitements aux exigences de protection des données.

Les téléviseurs connectés («smart TV» ou téléviseurs intelligents) sont de plus en plus prisés. Ils offrent à l'utilisateur une expérience télévisuelle augmentée, en permettant l'accès à des contenus en ligne proposés par des chaînes de télévision, des prestataires d'applications et des fabricants de téléviseurs. Les utilisateurs n'ont toutefois souvent pas conscience qu'un échange de données a lieu et que leurs informations sont transmises aux prestataires offrant ces contenus.

Sur la base de requêtes de citoyens, nous avons ouvert une procédure d'établissement des faits auprès d'un fabricant de téléviseurs intelligents. Dans notre examen, nous mettons l'accent sur les questions suivantes: quelles sont les données concernant l'utilisateur qui sont traitées par le fabricant? Comment les utilisateurs en sont-ils informés? Les utilisateurs peuvent-ils s'opposer à ces traitements de données?

Nous analysons actuellement les réponses fournies par le fabricant.

1.3.2 Vol de données chez Swisscom

Nous avons été informés par Swisscom d'un accès abusif aux données à la fin de l'année 2017. Environ 800'000 clients sont concernés.

Fin décembre 2017, Swisscom nous a informés qu'en automne de la même année les coordonnées (nom, prénom, adresse, date de naissance et numéro de téléphone) de quelque 800'000 clients de l'entreprise avaient été subtilisées. Les clients concernés sont principalement des particuliers ayant un numéro de téléphone mobile, mais également quelques clients du réseau fixe. Les malfrats ont réussi à accéder aux coordonnées des clients de Swisscom en subtilisant les droits d'accès de l'un des partenaires de distribution de Swisscom. Nous avons alors conseillé Swisscom en l'accompagnant dans son appréciation de la situation et dans les démarches que l'entreprise a effectuées pour réduire les risques subséquents et protéger le droit de ses clients d'être informés du traitement de données les concernant. Swisscom a procédé à une clarification des faits, pris les mesures de protection nécessaires et informé ses clients début février 2018 du vol des données, si bien que le PFPDT a pu clore

ce dossier sans devoir prendre formellement de mesures. Peu après, des tiers nous ont annoncé un éventuel nouvel accès indu à d'autres données d'un client. Nous avons alors demandé formellement à Swisscom de se prononcer sur cet incident et de nous fournir des informations détaillées sur le risque d'éventuels dommages liés directement au vol de données précité. Swisscom nous a alors immédiatement et clairement montré qu'il n'existait aucun lien – comme on aurait pu le craindre – entre cet incident et le vol de données précité. La documentation supplémentaire demandée à Swisscom va être analysée par le PFPDT.

1.3.3 Mise en place d'une preuve d'identité électronique (e-ID)

La mise en place d'une identité électronique (e-ID) doit servir en premier lieu à renforcer la sécurité juridique des échanges numériques. Nous avons d'une part suivi ce grand projet dans le cadre de la consultation législative, d'autre part accompagné deux initiatives privées.

La conception actuelle d'une identité électronique repose sur une répartition des tâches entre l'État et les particuliers, qui a été intensivement débattue dans le cadre de la consultation sur le projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID). Nous avons pris position sur ce projet de loi, avons formulé des commentaires portant sur la protection des données et continuons de suivre les travaux sur le projet.

Avant même l'achèvement de la base légale pour l'e-ID, deux conglomérats d'entreprises privées nous ont présenté des concepts étendus concernant la notion de fournisseur d'identité prévue par le projet de loi. Nous avons à cet égard adopté une position critique, mais constructive.

Au cours de nombreuses réunions avec ces entreprises, nous avons indiqué les instruments de travail servant, dès la phase de conception, à clarifier les risques des grandes applications numériques et leurs éventuels impacts sur les droits de la personnalité. Les entreprises que nous avons conseillées ont donc clairement conscience du fait qu'elles doivent également prévoir des mesures concrètes pour prévenir les atteintes à l'autodétermination informationnelle des personnes concernées.

Outre l'évaluation des risques, d'autres exigences de protection des données doivent être respectées dans les concepts relatifs à l'émission d'une e-ID. Ainsi, aucune contrainte directe ou indirecte ne doit être exercée pour l'acquisition et l'utilisation d'une e-ID. Au contraire, des solutions alternatives à l'enregistrement en ligne (processus de «sign-in») doivent être proposées pour permettre un accès analogue aux informations et aux services, sans tracasseries administratives ni préjudice économique. L'utilisation de l'e-ID ne doit pas être subordonnée à la communication d'un plus grand nombre de données personnelles que la solution alternative. Si le service ou les informations recherchées n'impliquent pas obligatoirement l'identification de la personne, par exemple pour l'acquisition d'un billet de train, l'accès doit pouvoir rester anonyme. Nous exigeons également que tous les aspects des traitements de données liés au concept d'e-ID, ainsi que les prescriptions réglementaires et dispositions d'utilisation sur lesquelles ils reposent, soient accessibles au public sous une forme compréhensible.

Les mesures techniques et organisationnelles doivent exclure toute possibilité d'utilisation abusive des données. Il convient en particulier de veiller à ce qu'aucun des acteurs impliqués ne dispose de plus d'informations que ce dont il a besoin pour accomplir la tâche qui lui a été attribuée dans le cadre du système général de répartition du travail.

Ces mesures et leur impact doivent être documentés et décrits en détail par les entreprises. Ce travail de documentation est la condition préalable à l'accompagnement des projets par nos équipes interdisciplinaires de juristes et d'informaticiens dans le cadre de notre activité de conseil. Tous les acteurs avec lesquels nous sommes en contact se sont déclarés favorables à cette procédure.

1.3.4 Arrêt du Tribunal fédéral concernant le droit d'accès aux données secondaires

Le Tribunal fédéral a confirmé la position adoptée par le PFPDT concernant le droit d'accès aux données secondaires de télécommunications. Sur demande, les fournisseurs de services de télécommunications doivent livrer toutes les informations en leur possession qui concernent l'auteur de la demande ou sont susceptibles d'être associées à celui-ci.

Par son arrêt du 2 mars 2018 (1C_598/2016), le Tribunal fédéral a rejeté le recours formé par six particuliers concernant l'enregistrement et la conservation des données secondaires de télécommunications. Par son même arrêt, il a confirmé le droit d'accès comme garantie de droit procédural, contre un traitement inapproprié des données.

Le PFPDT se penche depuis quelque temps sur la question des demandes de renseignements relatives aux données secondaires stockées par les fournisseurs de services de télécommunications. Nous avons constaté que ces sociétés refusent de donner des informations sur les données secondaires qui ne sont pas utilisées à des fins de facturation. Nous leur avons fait savoir à maintes reprises que le droit d'accès porte sur toutes les données secondaires et n'est pas limité à celles destinées à la facturation. Au vu de la procédure qui vient de s'achever, alors encore en cours, nous avons renoncé à soumettre le cas à une autorité judiciaire. Nous avons pu exposer notre position dans le cadre de la consultation. Elle a été confirmée par le présent arrêt du Tribunal fédéral.

Le droit d'accès fait partie intégrante des droits fondamentaux inscrits dans la Constitution et représente un élément central du droit de garder la maîtrise de ses données personnelles. À cet égard, il vise à garantir la protection de la personnalité, puisqu'il permet aux personnes intéressées de contrôler l'usage qui est fait des données les concernant recueillies dans un fichier, le but étant de vérifier et, le cas échéant, d'assurer l'application des principes et dispositions relevant de la protection des données.

Les fournisseurs de services de télécommunications craignent que suite à une demande de renseignements, les auteurs d'une telle demande aient accès à des informations sensibles sur d'autres utilisateurs raccordés au même réseau. Le Tribunal fédéral relève d'ailleurs que les demandes de renseignements constituent un abus si elles sont déposées par simple curiosité envers autrui. Un tel comportement ne saurait être assimilé à un droit car il serait en contradiction avec la raison d'être du droit d'accès. Dans une large mesure, il peut être remédié au risque d'abus que craignent certains par la mise en place de processus d'authentification adaptés au moyen de communication employé (réseau fixe, Internet, portable) qui permettent d'identifier l'utilisateur d'un raccordement.

1.4 Justice, Police, Sécurité

1.4.1 Surveillance de la correspondance par poste et télécommunication: révision des dispositions d'application

Au cours de la procédure de consultation des offices, nous avons pris position sur les ordonnances révisées de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Ces dernières réglementent les traitements de données effectués par le Service Surveillance de la correspondance par poste et télécommunication (SCPT) et détaillent les types de données que doivent fournir les fournisseurs de services de télécommunication.

En mars 2016, le Parlement a adopté la révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Les dispositions d'application ont dû à leur tour être entièrement révisées. Nous avons pris position une première fois sur les projets d'ordonnance en 2016 (cf. 24^e rapport d'activités 2016/2017, chiffre 1.4.2). À l'issue de la procédure de consultation, certaines divergences n'avaient pas été prises en compte, si bien que nous avons rendu une nouvelle prise de position. Celle-ci portait sur le stockage de l'adresse IP cible et du numéro de port cible lors d'un accès Internet avec le protocole NAT (Network Address Translation), la recherche par champ d'antennes et les ressources d'adressage dans les échanges d'e-mails.

Nous avons exigé une réglementation claire, prévoyant que l'identification de l'abonné par utilisation de la procédure carrier-grade NAT (traduction d'adresses de réseau au niveau du fournisseur; cgNAT) au niveau du fournisseur d'accès ne devait pas impliquer le stockage des données de connexion cibles. Dans la procédure cgNAT, les usagers du réseau exploité par le fournisseur d'accès se voient attribuer une adresse IP privée, valable uniquement à l'intérieur de ce réseau. Lorsque ces usagers accèdent à Internet, leurs adresses IP privées sont converties, c'est-à-dire traduites, à l'extrémité du réseau du fournisseur d'accès, en une adresse IP source publique commune (un grand nombre d'utilisateurs utilisent simultanément une même adresse IP publique). La différenciation des nombreuses connexions Internet est opérée au moyen de numéros de port. Cette traduction des adresses doit être effectuée pour chaque paquet IP entrant et sortant. Dans une procédure non déterministe, l'équipement utilisé pour la traduction (routeur) stocke dans une table d'attribution, pour chaque connexion Internet (contexte), le timbre horodateur, la source et la destination de la connexion (adresses IP et numéros de port), l'adresse

IP privée et le numéro de port de l'utilisateur, ainsi que le type de protocole de transport. Nous avons proposé que l'ordonnance prescrive l'utilisation de la procédure NAT déterministe, dans laquelle les adresses et les numéros de port sont traduits au moyen d'un algorithme qui permet de recalculer par la suite l'adresse et le numéro de port initiaux. Le fournisseur d'accès n'a par conséquent pas besoin de sauvegarder les adresses IP et les numéros de port de destination des différentes connexions pour identifier les usagers. Notre exigence n'a été que partiellement retenue: il est précisé dans les explications qu'il convient, à des fins de respect du droit de la protection des données, d'implémenter des procédures ne nécessitant pas le stockage des données de connexion cibles, ce dernier étant dans ce cas à proscrire.

Selon l'ordonnance, une recherche par champ d'antennes peut être demandée sur une durée maximale de deux heures pour une cellule d'antenne mobile déterminée ou un point d'accès WLAN déterminé. L'une de nos préoccupations concernait la limitation de la recherche par champ d'antennes aux cellules de téléphonie mobile. Nous avons également insisté sur le fait que les recherches par champ d'antennes devaient se limiter au nombre de suspects défini par l'autorité de poursuite pénale. Nous avons déjà souligné ces points lors de la consultation des offices concernant la loi fédérale. Si les données de toutes les personnes présentes en un lieu donné à un moment donné sont transmises, cela peut induire une atteinte disproportionnée aux droits fondamentaux de nombreux individus, voire s'apparenter dans un cas extrême à une recherche par quadrillage systématique, ce qui n'est pas prévu par la loi. Nos exigences n'ont pas été prises en compte, si bien que les tribunaux des mesures de contrainte, lors de leur examen du critère de proportionnalité des recherches par champ d'antennes, peuvent influencer uniquement sur la durée et le nombre de cellules, mais ne peuvent pas fixer un effectif de personnes ciblées pour circonscrire l'étendue des données collectées.

Concernant les dispositions d'exécution portant sur la surveillance des ressources d'adressage, le champ d'application a été étendu aux e-mails. Il s'agit de la surveillance des échanges d'e-mails entre le client d'un fournisseur de service de courrier électronique et une autre adresse e-mail «étrangère», non gérée par ce fournisseur. En fonction des techniques mises en œuvre, cet instrument peut conduire, au-delà de l'accès prévu par la loi aux données secondaires, à une surveillance illégale des contenus. Nous avons exigé une description précise des modalités d'application de ce type de surveillance. Cette description a été intégrée dans les explications, mais pas directement dans l'ordonnance. Il a été précisé que la surveillance des ressources d'adressage dans les e-mails n'était autorisée que pour surveiller les opérations sur les serveurs de messagerie, comme les envois et réceptions d'e-mails, mais pas pour accéder à des boîtes mails «étrangères». De plus, l'analyse doit porter uniquement sur les éléments d'adressage de l'enveloppe SMTP (données techniques concernant la transmission des e-mails).

Comme le contenu des ordonnances est très technique et, comme nous l'avons évoqué, pas toujours suffisamment détaillé, il a été décidé de publier des explications accompagnant les différentes dispositions d'application. Cette décision va dans le sens de la procédure que nous préconisons pour améliorer la compréhension des différentes dispositions.

1.4.2 Reconnaissance faciale à l'aéroport

Le Corps des gardes-frontière prévoit de mettre en place et d'exploiter à l'aéroport de Genève un système de contrôle automatique des passeports avec reconnaissance faciale.

Au cours de l'année sous revue, le contrôle automatique des passeports avec reconnaissance faciale a été testé à l'aéroport de Zurich. Ce test, mené par la police aéroportuaire de Zurich, relevait de la compétence du Préposé à la protection des données du canton de Zurich. Le Corps des gardes-frontière prévoit d'utiliser les mêmes équipements à partir du second semestre 2018 à l'aéroport de Genève. Nous avons contacté le Corps des gardes-frontière pour être informés du projet. Nous allons continuer de suivre sa mise en œuvre pour nous assurer que le droit de la protection des données est respecté.

1.4.3 Loi fédérale sur les précurseurs de substances explosibles et loi fédérale sur les mesures policières de lutte contre le terrorisme

Dans le cadre de la consultation des offices et lors d'une séance avec la direction de l'Office fédéral de la police (fedpol), nous avons émis un grand nombre de remarques au sujet des deux projets législatifs mentionnés en titre. Fedpol a tenu compte d'une partie de nos remarques.

En ce qui concerne le projet de loi fédérale sur les précurseurs de substances explosibles, fedpol a tenu compte de toutes nos remarques excepté celle concernant l'utilisation du numéro AVS (NAVS13). Nous avons donc demandé à fedpol de mentionner dans la proposition au Conseil fédéral la divergence suivante: «Tant que le Conseil fédéral n'a pas montré dans un concept de quelle manière il est possible de faire face aux risques liés à l'utilisation du NAVS13 en tant qu'identifiant des personnes unique et de quelle manière la protection des données dans le cadre de l'utilisation de numéros d'identification de personnes peut être améliorée (cf. Postulat 17.3968 de la Commission des affaires juridiques du conseil national), le PFPDT est opposé à toute utilisation du NAVS en dehors du secteur des assurances sociales et est de l'avis que le présent projet de loi doit renoncer à traiter le NAVS.»

Quant au projet de loi fédérale sur les mesures policières de lutte contre le terrorisme, les divergences avec fedpol sont plus nombreuses.

Le droit de police de la Confédération est ancré dans différentes lois. Cela ne permet pas d'avoir une vue d'ensemble claire sur les différents traitements de données personnelles. Le présent projet aggrave cette situation. Nous exigeons donc l'élaboration d'une loi sur les activités de police de la Confédération comme cela existe au niveau des cantons. De plus, il n'est pas clair dans quel système ou sous-système d'information les données relatives aux mesures policières de lutte contre le terrorisme seront traitées.

Le projet prévoit de nouveaux accès en ligne pour le Secrétariat d'Etat aux migrations (SEM) et aux corps des gardes-frontière à certains systèmes d'information de fedpol. Ces accès concernent des données de police judiciaire ou des données relatives à des analyses criminelles. Ces données sont très sensibles et certaines ne sont pas encore sûres. L'accès à de telles données par les autorités de migrations et de contrôle aux frontières doit s'effectuer par le biais de l'entraide administrative et non pas par un accès en ligne. De cette manière fedpol pourrait réduire au nécessaire la dissémination de ces données.

Pour terminer, nous avons indiqué la nécessité de définir les compétences de la police des transports des CFF avant de lui attribuer un accès au système de recherches informatisées de police (RIPOL).

1.4.4 Groupe de travail sur la révision de la loi sur les profils d'ADN

Nous avons participé au groupe de travail sur la révision de la loi sur les profils d'ADN. Dans ce cadre, nous avons indiqué que nous ne sommes pas convaincus de l'utilité de modifier la loi sur les profils d'ADN.

Le groupe de travail s'est penché sur trois thèmes principaux: Le premier de ces thèmes traite de la création des bases légales nécessaires afin que les autorités de poursuite pénale soient autorisées à poursuivre de façon ciblée les auteurs d'actes de violence graves tels qu'un meurtre ou un viol en procédant à l'analyse de séquences codantes de l'ADN, qui permet d'identifier des caractéristiques personnelles. Nous avons mentionné que cette possibilité d'analyser les séquences codantes doit dans tous les cas faire l'objet d'un cadre juridique stricte (limitation à des cas exceptionnels et décision par une autorité judiciaire).

Le deuxième thème concerne l'évaluation des différents délais de conservation des profils d'ADN. Nous estimons que la législation actuelle est proportionnée et tient suffisamment compte des exigences de la poursuite pénale en ayant des délais d'effacement différenciés et équilibrés. L'idée de trouver un seul délai de conservation des profils d'ADN ne respecte pas le principe de proportionnalité et ne tient pas compte des exigences spécifiques contenues dans le droit pénal des mineurs. La solution pourrait être un système avec deux délais, un long et un court.

Le dernier thème a trait à d'autres éléments nécessitant une révision de la loi comme la durée de conservation du matériel biologique dans les laboratoires ou les recherches familiales. Par ces dernières, une personne parente de l'auteur présumé se retrouve impliquée dans une procédure uniquement par ce lien de parenté. La loi ne confère pas expressément la possibilité à l'autorité pénale de comparer les profils ADN à l'intérieur d'une banque de données ADN, dans le but de trouver des profils ADN proches. En plus, les recherches familiales entrent en conflit avec le droit de refuser de témoigner au sens des articles 168 et suivants du Code de procédure pénale. Si le législateur souhaite autoriser ces recherches familiales, des réglementations strictes avec des critères précis sont nécessaires. Dans le cadre de la révision de la loi sur les profils d'ADN, les recherches familiales devraient être intégrées dans cette révision législative. Nous interviendrons afin que la réglementation respecte les principes généraux de protection des données, notamment la

proportionnalité. Une recherche familiale ne devra intervenir que dans des cas de crimes particulièrement graves et qu'en dernier recours (recherches infructueuses dans les banques de données suisses et étrangères).

1.4.5 Collaboration dans l'espace Schengen

En 2017, nous avons participé aux réunions des groupes de coordination de contrôle des systèmes d'information SIS II, VIS et Eurodac. Nous étions également représentés lors des réunions du sous-groupe de travail «Border, Travel & Law Enforcement» (BTLE), mis en place par le groupe de travail sur la protection des données de l'Union européenne («article 29»). Enfin, en février/mars 2018 a eu lieu l'évaluation Schengen pour la Suisse.

Groupes de coordination de contrôle des systèmes d'information SIS II, VIS et Eurodac

Cette année encore, nous avons pris part aux réunions des trois groupes de travail, qui se sont déroulées successivement en juin et en novembre 2017 à Bruxelles. Des résumés de ces réunions, des rapports d'activités et d'autres informations sur ces groupes sont disponibles en anglais, en français et en allemand sur les sites www.sis2scg.eu, www.visscg.eu et www.eurodacscg.eu. Depuis novembre 2017, nous assurons la présidence du groupe de coordination de contrôle VIS. Le secrétariat est assuré par le Contrôleur européen de la protection des données.

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

Au cours de l'année sous revue, nous avons participé à cinq réunions du sous-groupe de travail, qui ont notamment porté sur la directive UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par la police et les autorités de poursuite pénale (directive UE 2016/680) et sur la révision de l'accord Privacy Shield UE-États-Unis. La directive précitée comprend, dans le contexte de sa transposition dans le droit national, quelques points délicats au regard du droit de la protection des données. La question des autorités relevant de son champ d'application, en particulier, a fait l'objet de discussions approfondies, de même que la délimitation avec le Règlement général sur la protection des données. Le groupe de travail «article 29» a publié à la fin de l'année 2017 une recommandation («Opinion»), consultable à l'adresse http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178 (en anglais). La préparation et l'analyse de la première révision annuelle de l'accord Privacy Shield UE-États-Unis ont également été discutées

en détail. Nous avons suivi les travaux de près et avons pris part à la révision en qualité d'observateur (cf. chiffre 1.8.1 du présent rapport). Deux rapports ont été publiés à ce sujet, respectivement par la Commission européenne (cf. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619) et par le groupe de travail «article 29» (cf. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610114). Les deux organes se sont félicités du renforcement de la collaboration avec les autorités américaines. Des critiques ont été formulées concernant le volet commercial, notamment au sujet de l'activité de contrôle indépendant du côté du partenaire américain, jugée encore insuffisante. Dans le domaine de la sécurité nationale, la vacance de certains postes, le manque de clarté des bases législatives et la collaboration parfois insuffisante des différentes autorités de contrôle ont également été soulignés.

Évaluation Schengen de la Suisse dans le domaine de la protection des données

En 2018, la mise en œuvre et l'application de l'acquis de Schengen par la Suisse, en tant que membre associé, ont été contrôlées pour la troisième fois. L'évaluation, qui est menée à un intervalle maximum de cinq ans, porte sur l'ensemble des domaines de la collaboration Schengen: gestion des frontières extérieures (aéroports), retour/rapatriement, système d'information Schengen SIS II/SIRENE, politique commune en matière de visas, coopération policière et traitement des données à caractère personnel. Du 26 février au 23 mars 2018, des équipes composées d'experts des États membres de l'espace Schengen et de la Commission européenne ont effectué plusieurs visites sur site, notamment auprès de notre autorité et de celles du canton de Lucerne. Les résultats de l'évaluation pourront éventuellement aboutir à des recommandations adressées à la Suisse. Les travaux pour la préparation et l'exécution de l'évaluation ont été coordonnés par l'Office fédéral de la justice (OFJ), en collaboration avec la Direction des affaires européennes (DAE). Nous avons participé activement aux travaux de l'évaluation Schengen dans le domaine de la protection des données.

La collaboration Schengen repose sur la confiance et l'assistance mutuelles. Un mécanisme d'évaluation efficace, à même d'identifier les possibilités d'amélioration dans la mise en œuvre et l'application de l'acquis de Schengen, est donc dans l'intérêt de tous les États membres de l'espace Schengen.

1.4.6 Contrôle des visas Schengen au SEM

En 2017, nous avons examiné les traitements de données effectués au Secrétariat d'État aux migrations (SEM) en relation avec les visas Schengen et procédé à des contrôles sur place.

Les autorités de protection des données des États membres de l'espace Schengen sont tenues, de par le droit européen, de contrôler au moins tous les quatre ans les traitements de données opérés par leurs autorités nationales concernant les visas Schengen. En 2017, nous avons contrôlé le SEM. Nous avons examiné les traitements de données effectués dans le système suisse d'information sur les visas (ORBIS) ainsi que les échanges de données entre l'interface nationale N-VIS et le système central d'information sur les visas de l'UE (C-VIS). Notre procédure d'établissement des faits s'est limitée aux visas Schengen. Nous n'avons pas contrôlé l'accès aux données par les autorités de poursuite pénale. Nous avons au préalable interrogé le SEM concernant l'attribution des accès, la formation des personnes disposant d'accès, les traitements de données, les droits des personnes concernées, ainsi que la sécurité et la conservation des données. Par ailleurs, nous avons effectué à l'automne 2017 un contrôle sur place. Au moment de la rédaction du présent rapport, notre procédure d'établissement des faits n'était pas encore achevée.

1.4.7 Mise en œuvre Schengen: contrôle des signalements prononcés auprès du SEM

Dans le cadre des accords d'association à Schengen, nous avons procédé à un contrôle des signalements prononcés aux fins de non-admission ou d'interdiction de séjour auprès du SEM en tant qu'utilisateur final du Système d'information Schengen (SIS).

L'objectif de ce contrôle consistait en particulier à vérifier que le SEM respecte les exigences légales de protection des données concernant l'introduction de signalements relatifs à l'article 24 du Règlement SIS II (conditions auxquelles sont soumis les signalements introduits aux fins de non-admission ou d'interdiction de séjour), de l'application de l'article 25 de la Convention d'application de l'Accord de Schengen (CAAS) (titres de séjour et signalement aux fins de non-admission) ainsi que de la législation suisse d'application (en particulier la loi fédérale sur les systèmes d'information de police de la Confédération ; LSIP) et l'ordonnance sur la partie nationale du système d'information Schengen (N-SIS) et sur le bureau SIRENE (ordonnance N-SIS).

En raison de l'importance et de l'ampleur des traitements de données personnelles effectués dans le SIS en Suisse, nous avons axé notre contrôle sur les traitements de données effectués dans le SIS, plus précisément sur les signalements prononcés sur la base de la loi fédérale sur les étrangers (LEtr) (signalements introduits aux fins de non-admission ou d'interdiction de séjour) et de l'utilisation du SIS par le SEM. En revanche, le contrôle ne couvrait pas les accès et traitements des données de l'Office fédéral de la police (fedpol) et du bureau SIRENE de même que ceux des autorités cantonales, lesquelles sont soumises à la surveillance des préposés cantonaux à la protection des données.

Nous avons dans un premier temps envoyé au SEM un questionnaire et procédé à une analyse de la documentation reçue. Nous avons également procédé à un contrôle sur place. Ce contrôle a porté sur différents points. Il nous a permis de voir de quelle manière les collaborateurs du SEM ont accès aux données du SIS, quelle est la procédure en matière de signalements aux fins de non-admission ou d'interdiction de séjour et quelles processus ont été mis en place en cas de traitement illicite ou lorsqu'il apparaît que des données incorrectes figurent dans le SIS. Nous avons également vérifié les profils des collaborateurs du SEM ayant un droit d'accès au SIS. L'analyse des fichiers de journalisation n'a pas été effectuée lors de ce contrôle mais fera plus spécifiquement l'objet d'un prochain contrôle auprès du SEM de même que d'autres utilisateurs fédéraux. Nous avons également demandé au fedpol de nous fournir des compléments d'informations relatifs aux traitements des données du SIS.

Nous sommes arrivés à la conclusion que les traitements de données effectués en Suisse remplissent les conditions spécifiées dans le Règlement SIS II, dans la CAAS, ainsi que dans la législation suisse d'application. Nous n'avons ainsi pas eu à formuler de recommandation.

1.5 Santé et recherche

1.5.1 Dossier électronique du patient

La mise en place du dossier électronique du patient se poursuit. Le besoin de conseil et d'information en matière de protection des données est élevé et mobilise une part considérable des ressources de notre autorité.

Au cours de l'année sous revue, le Préposé et ses collaborateurs ont participé à des tables rondes sur le dossier électronique du patient, effectué des présentations auprès d'associations et d'entreprises, été entendus par des organes de partis politiques, conseillé les exploitants de communautés de référence, mené des discussions avec les autorités cantonales de protection des données et répondu à de nombreuses requêtes de citoyens sur ce thème. Ces activités ont fortement sollicité les ressources de notre autorité. Le travail de conseil peut se limiter à une simple communication de renseignements sur le consentement, mais prend parfois la forme d'explications détaillées dans le domaine, par exemple, de la médecine de laboratoire. Des connaissances approfondies dans le domaine de la santé sont alors nécessaires et seuls quelques-uns de nos collaborateurs spécialisés sont en mesure de répondre à ces requêtes. Ces collaborateurs spécialisés seront également très sollicités dans les prochaines phases du projet et commenceront leurs activités de contrôle lors du lancement de la phase productive (prévu pour 2020).

1.5.2 Projet statistique BAGSAN

L'anonymat des assurés est un aspect hautement prioritaire du projet BAGSAN de l'Office fédéral de la santé publique (OFSP). Dans le cadre de l'accompagnement du projet, nous avons fait des propositions concrètes pour réduire les risques de réidentification et d'utilisation abusive des données en interne.

Le projet statistique BAGSAN, fondé sur les données individuelles détenues par les assureurs-maladie, est mené par l'OFSP. Sur la base des résultats des premiers relevés de données, nous avons recommandé de nouvelles mesures visant la réduction du risque de réidentification. Pour que les données soient considérées par notre autorité comme des données anonymisées et non plus comme des données personnelles au sens de la loi sur la protection des données, la réidentification ne doit plus être possible qu'au prix d'un effort disproportionné. Nous avons également proposé des mesures pour réduire le risque d'utilisation abusive des données par des personnes disposant de droits d'accès et de modification étendus. Ce risque est également qualifié dans

la pratique de «risque d'administrateur». Nous avons proposé de répartir les droits entre plusieurs personnes, qui devraient agir simultanément pour obtenir du système l'autorisation d'accès. Nos propositions ont été accueillies favorablement par l'OFSP. Avant de passer aux phases ultérieures de ce projet, impliquant des jeux de données complets sur chaque personne assurée, un temps d'arrêt a été décidé pour laisser le temps à la discussion politique de suivre son cours. Selon une initiative adoptée par le Parlement, les assureurs-maladie ne doivent pas transmettre de données individuelles pour les besoins du projet BAGSAN. Jusqu'à nouvel ordre, donc, les assureurs consultés par l'OFSP ne fournissent pas de jeux de données complets. Dans le cadre de l'évaluation politique du projet BAGSAN, nous conseillons également les commissions parlementaires compétentes, ce qui mobilise des ressources juridiques et techniques considérables.

1.5.3 Davantage de transparence pour les patients en cas d'externalisation du traitement des factures de médecins

Nous avons invité les prestataires Swisscom Health et Caisse des Médecins à améliorer la transparence des informations fournies aux patients sur leurs sites Internet.

Dans le cadre du traitement des factures et de la gestion des créances, les prestataires Caisse des Médecins et Swisscom Health traitent de grandes quantités de données sur les patients. Il s'agit de données administratives concernant les fournisseurs de prestations médicales et les patients et de données sur la santé qui sont nécessaires à l'établissement des factures. Pour que les patients concernés puissent s'informer des modalités de traitement de leurs données, nous avons invité les deux prestataires à mettre en ligne sur leurs sites Internet les contrats modèles, les contrats de produits, les conditions commerciales générales et les règlements relatifs au traitement des données dans leur version actuelle. Les deux prestataires ont réagi favorablement à notre requête: la Caisse des Médecins a publié les informations demandées dans une nouvelle rubrique intitulée «Infos patients». Swisscom Health nous a quant à elle soumis un concept de mise en œuvre préalable et a publié les premières informations sur son site internet. La transparence des prestataires mandatés est importante, car ils occupent une position de plus en plus décisive dans le traitement des données. Comme le montre également l'affaire de

l'entreprise EOS (cf. chiffre 1.8.2 du présent rapport), les mandants perdent de plus en plus la main sur l'organisation de la relation contractuelle et ainsi le contrôle sur le traitement des données. Comme le souligne également le cas EOS, les fournisseurs de prestations médicales, en tant que mandants, supportent l'entière responsabilité de la protection et la sécurité des données lors de leur traitement par un prestataire externe.

1.5.4 TARPSY, nouvelle structure tarifaire unique: extension des attributions des services de réception des données

Depuis le 1^{er} janvier 2018, les traitements psychiatriques stationnaires sont régis par la structure tarifaire TARPSY. Désormais, les factures établies selon le modèle TARPSY transitent par les services de réception des données des assurances maladie, comme c'est le cas pour les factures SwissDRG.

La nouvelle structure tarifaire TARPSY sert au paiement de tous les traitements psychiatriques stationnaires au moyen des forfaits par cas liés aux prestations, comme c'est le cas depuis longtemps pour les prestations hospitalières stationnaires en médecine somatique aiguë, conformément au modèle de facturation SwissDRG. Désormais, les fournisseurs de prestations du domaine de la psychiatrie stationnaire doivent aussi transmettre les factures TARPSY au service de réception des données certifié de l'assurance-maladie concernée – comme elles le font pour les factures SwissDRG –, ce qui correspond à une extension des attributions des services de réception des données, qui doivent dès lors traiter ce nouveau type de factures. Nous allons suivre de près cette mise en œuvre par les assurances-maladie pour nous assurer que les choses sont faites correctement.

1.5.5 La SUVA transmet des données sur les assurés à des fins de recherche

La SUVA (Caisse nationale suisse d'assurance en cas d'accidents) utilise des données sur les assurés pour des projets de recherche, impliquant parfois une transmission des données à des tiers. L'enquête préliminaire a révélé que la SUVA devait procéder à des améliorations en relation avec l'information de ses assurés et l'exercice par ces derniers de leur droit d'opposition.

En mars 2017, un médecin nous a signalé que la SUVA mettait apparemment des données concernant ses assurés à la disposition de tiers pour une utilisation dans des projets de recherche. Les personnes concernées ont la possibilité de refuser l'utilisation de leurs données et sont informées de ce droit d'opposition (droit de veto dans la terminologie de la SUVA) par leur médecin traitant. Une brochure contenant des informations sur le droit de veto est également disponible dans les cliniques de réadaptation et les agences de la SUVA, mais elle n'est apparemment consultée que par une minorité des assurés. Le document peut aussi être consulté sur le site Internet de la SUVA, mais dans la rubrique «Informations destinées aux médecins», qui s'adresse au personnel médical.

À l'occasion d'une rencontre, la SUVA nous a exposé en détail la procédure qu'elle applique à l'examen des demandes de soutien pour des projets de recherche internes et externes, ainsi que les modalités d'exercice du droit de veto par les assurés. Le soutien apporté par la SUVA aux projets de recherche est avant tout financier; l'utilisation ou la transmission de données sur les assurés dans le cadre des projets qu'elle appuie sont relativement rares. Dans tous les cas, les données sont anonymisées avant d'être transmises. Les données génétiques ne sont pour le moment pas concernées.

Selon nous, il existe un besoin d'amélioration au niveau de l'information des assurés par la SUVA, que ce soit au niveau du contenu de l'information ou de la façon dont les informations sur le droit d'opposition sont diffusées. La majorité des assurés ignorent que leurs données peuvent être utilisées dans des travaux de recherche, bien que leur médecin traitant soit censé les en informer. Par conséquent, ils n'ont pas non plus connaissance de leur possibilité d'exercer un droit d'opposition.

Il convient de communiquer clairement la possibilité d'une utilisation des données sur les assurés à des fins de recherche. Les informations à ce sujet doivent être facilement accessibles. De plus, de notre point de vue, le processus interne d'anonymisation des données doit également être amélioré.

La SUVA nous a affirmé qu'elle mettrait en place les adaptations nécessaires au cours du premier trimestre 2018 et nous a soumis un concept pour examen.

1.6 Assurances

1.6.1 Procurations dans le domaine des assurances d'indemnités journalières de maladie

Les procurations demandées par les assureurs d'indemnités journalières de maladie déconcertent ou inquiètent souvent les malades. Nous recevons donc de nombreuses demandes d'assurés souhaitant savoir si ces procurations sont légales.

Les assurances d'indemnités journalières de maladie permettent aux employeurs de couvrir le risque d'obligation de payer le salaire à des collaborateurs en arrêt-maladie prolongé. À la survenance d'un cas de maladie, l'assureur doit déterminer son obligation de verser des prestations et l'étendue de ces prestations. Comme bon nombre de personnes ou services détenant les informations nécessaires est tenu à une obligation légale ou contractuelle de garder le secret, l'assureur demande une procuration pour pouvoir se procurer les informations dont il a besoin. La portée de cette procuration est souvent peu claire pour les personnes concernées, qui ne comprennent pas pourquoi elles doivent autoriser les médecins, les hôpitaux, les autres assureurs, leur employeur, les services sociaux ou l'administration fiscale à communiquer des données sur leur personne. De plus, elles n'ont pas non plus toujours conscience d'être tenues, de par l'obligation de réduction du dommage, de délivrer cette procuration. Du point de vue de la protection des données, il est essentiel que la procuration soit limitée à un événement concret et aux informations qui sont pertinentes pour sa clarification. La procuration ne doit en aucun cas être un blanc-seing. De plus, les services sollicités par l'assureur sont également tenus de respecter le principe de la proportionnalité dans leur divulgation de données. Ils ne doivent communiquer à l'assureur que les informations portant concrètement sur le cas en question. Vous trouverez des explications sur ce thème sur notre site Internet, à l'adresse : www.leprepose.ch, Protection des données – Assurances – Assurances-maladie/accidents – Procurations.

1.6.2 Système d'information pour la lutte contre la fraude à l'assurance

Nous conseillons l'Association suisse d'assurances dans la mise en place d'un système central d'information pour la lutte contre la fraude à l'assurance.

Pour la mise en place de ce système, l'ASA fait appel à des experts ayant participé à la création et à l'exploitation du système de renseignement et d'information du secteur des assurances en Allemagne. Nous conseillons à la fois l'ASA et les experts sur les questions relatives à la protection et à la sécurité des données.

1.6.3 Externalisation de tâches des assurances-maladie à des prestataires de services externes à la branche

Dans le domaine de l'assurance-maladie, on assiste de plus en plus à l'externalisation – à des prestataires de services externes à la branche – de tâches qui étaient auparavant effectuées par les assurances-maladie elles-mêmes. Nous avons examiné un cas dans lequel le mandataire a ouvert et traité la correspondance entre des assurés et leur assurance-maladie.

Dans le domaine de l'assurance-maladie, la tendance est manifestement à l'externalisation de tâches classiques que les assurances-maladie confient à des tiers dont l'activité principale ne concerne pas forcément le domaine de la santé. De toute évidence, les assurances-maladie espèrent ainsi obtenir des gains d'efficacité se traduisant par des réductions de coûts et de temps.

Nous avons découvert un cas où la Caisse de Santé EGK a confié l'ouverture et la numérisation de lettres à la Poste Suisse, plus précisément à sa filiale Swiss Post Solutions. Le traitement de la correspondance des assurés par un intermédiaire qui n'est pas considéré, pour l'opinion publique, comme un fournisseur de prestations dans le secteur de la santé, a suscité le mécontentement de bon nombre d'assurés. Cette situation soulève notamment une série de questions concernant le respect des prescriptions régissant la protection des données. C'est la raison pour laquelle nous avons mené des investigations préliminaires auprès de la Caisse de Santé EGK durant l'année sous revue. Nos investigations ont révélé que le traitement externalisé de la correspondance postale des assurés est effectué avec soin et que le respect du secret postal et des secrets privés, mais aussi des normes actuelles en matière de sécurité des données, est garanti. Qui plus est, la Caisse

de Santé EGK a informé ses assurés de manière ouverte et transparente au sujet des changements concernant le traitement de la correspondance postale. Par conséquent, nous n'avons constaté aucune irrégularité sous l'angle du droit de la protection des données.

1.6.4 Applications de santé et programmes bonus des assurances-maladie

Durant l'année sous revue, nous nous sommes intéressés à plusieurs applications de santé et programmes bonus proposés par des assurances-maladie. Nous avons cherché à savoir non seulement si les assurés mettent librement leurs données de santé à la disposition des assurances, mais également si les prescriptions en matière de protection des données et de sécurité sont respectées. Nous avons entamé une procédure d'établissement des faits qui porte sur le programme bonus «Helsana+».

Durant l'année sous revue, nous avons rendu visite à plusieurs assureurs pour qu'ils nous fournissent des informations de première main sur les nouveaux programmes bonus, de même que sur les applications de santé et sur les plateformes qui leur sont consacrées, mais aussi pour qu'ils nous présentent et nous expliquent les produits en question.

Nous avons examiné l'application de santé «myStep», proposée par la CSS et le programme bonus «BENEVITA», proposé par SWICA. Ces produits ont ceci en commun que les caisses-maladie récompensent leurs assurés qui adoptent un mode de vie sain et actif en leur accordant des remises de prime dans les assurances complémentaires. Dans le cas de «myStep», les assurés sont encouragés à faire davantage d'exercice physique au quotidien grâce à un podomètre électronique, tous les pas effectués étant comptabilisés sur le compte myStep et peuvent être consultés sur le portail myCSS. Les assurés reçoivent une «rémunération pour les pas effectués», laquelle peut être versée par l'intermédiaire du compte «santé». L'assureur a toutefois l'interdiction de transmettre à des tiers les données concernant les pas effectués. Le programme bonus «BENEVITA» de SWICA récompense également l'activité physique, les assurés se voyant offrir sur la plateforme santé BENEVITA une série de prestations comme des conseils de santé personnalisés et des activités de coaching par des experts. Les assurés peuvent collecter des points bonus et ainsi faire baisser leurs primes dans les assurances complémentaires. Là aussi, les données de santé ne sont pas transmises à des tiers, par exemple à des fins publicitaires.

En octobre 2017, nous avons ouvert une procédure d'établissement des faits à l'égard de la caisse-maladie Helsana. Il nous a notamment fallu déterminer si cette dernière procède au traitement de données personnelles issues de l'assurance de base dans le cadre du programme bonus «Helsana+» étant donné qu'il s'agit du premier programme bonus auquel ont aussi accès les assurés qui ne disposent que de l'assurance de base. Le bonus a des incidences à tout le moins indirectes sur le niveau des primes de l'assurance de base. Après la clôture de la procédure, nous avons recommandé à Helsana Assurances complémentaires SA de mettre un terme à ce traitement de données de l'assurance de base et de cesser le traitement de données visant à calculer et à effectuer des remboursements sous forme pécuniaire pour les clients qui ne disposent que de l'assurance de base auprès d'Helsana (cf. nos communiqué et recommandation).

1.7 Secteur du travail

1.7.1 Gestion électronique du recrutement: conclusion de la procédure d'établissement des faits

Dans le cadre de la procédure d'établissement des faits concernant la gestion électronique du recrutement, une solution a pu être trouvée avec le Service de renseignement de la Confédération (SRC) pour la conservation et la suppression des informations contenues dans les dossiers de candidature électroniques.

Comme d'autres services, le Service de renseignement de la Confédération (SRC) recrute du personnel sur dossier de candidature électronique. Dans le cadre d'une procédure d'établissement des faits, nous avons constaté que la pratique du SRC concernant la conservation et la suppression des dossiers de candidature n'était pas entièrement conforme aux prescriptions légales. En concertation avec le Département fédéral de la défense, de la protection de la population et des sports (DDPS), une solution consensuelle a pu être trouvée, qui répond aux besoins spéciaux du SRC tout en garantissant la protection de la personnalité des candidats.

1.7.2 Un départ réussi en cas de résiliation des rapports de travail

Tout employeur devrait, dans un souci de transparence, édicter un règlement régissant l'utilisation des moyens informatiques par son personnel, et y indiquer les droits et les devoirs de chacun. Cette façon de faire permettrait d'éviter des conflits pendant les rapports de travail et à l'issue de ces derniers, tout en contribuant à ce que les départs se fassent de façon ordonnée.

Nous avons reçu de nombreuses questions orales et écrites émanant d'employés et d'employeurs sur la manière de procéder correctement, sur plan juridique, quand il s'agit de bloquer des moyens informatiques comme un compte de messagerie électronique ou l'accès à un serveur une fois que quelqu'un a décidé de quitter son emploi : à quoi faut-il veiller lors du blocage d'un compte de messagerie électronique? Dans quels délais doit-on bloquer l'accès au serveur et les mots de passe? Quelles sont les règles applicables aux données privées qui appartiennent à l'employé, notamment les courriels, photos et textes à caractère privé?

Nous avons conseillé aux employeurs de consigner les principes applicables dans un règlement intérieur régissant l'utilisation des moyens informatiques, de le distribuer à leurs employés et d'organiser des formations destinées à approfondir les connaissances en la matière. En résumé, nos recommandations sont les suivantes:

- avant son départ, l'employé devrait transmettre les dossiers et courriels en cours à la personne désignée par l'employeur et les quittancer;
- l'employé sur le départ devrait avoir la possibilité de sauvegarder ses courriels privés et d'autres documents sur des supports privés tels que des clés USB, mais aussi de les effacer des serveurs de l'employeur;
- au plus tard le dernier jour de travail, le compte de messagerie électronique de l'employé sur le départ et tous les autres comptes informatiques devraient être bloqués, puis effacés après un certain laps de temps;
- en cas de décès, le compte de messagerie électronique du défunt devrait être bloqué immédiatement, et les données qu'il contient devraient être sauvegardées. Ensuite, les courriels privés du défunt et toutes ses autres données à caractère privé devraient être triés en présence de ses proches selon le principe des quatre yeux;
- les personnes envoyant des courriels à l'adresse bloquée devraient recevoir une réponse automatique leur indiquant que l'adresse du destinataire n'est plus valable. La réponse automatique devrait contenir une adresse de remplacement permettant de contacter l'entreprise. Le message de l'expéditeur ne devrait pas être transmis automatiquement à une autre adresse électronique de l'entreprise.

L'observation de ces principes contribuera grandement au respect de la sphère privée et des secrets d'affaires des partenaires contractuels.

1.7.3 Géolocalisation de collaborateurs

Les appareils de navigation embarqués dans les véhicules de fonction et d'autres appareils avec fonction GPS semblent être utilisés de plus en plus souvent pour la surveillance de collaborateurs. Au cours de l'année sous revue, nous avons reçu plusieurs requêtes de personnes concernées. Ce type de surveillance n'est autorisé que dans le respect des conditions-cadres tant du droit sur la protection des données que du droit du travail.

Plusieurs personnes nous ont contactés sur notre hotline pour nous signaler qu'elles étaient confrontées dans leur travail à une surveillance par le biais d'appareils de navigation ou d'autres systèmes de localisation. Il s'agissait pour la plupart de collaborateurs de services externes, utilisant des véhicules de fonction déjà équipés d'appareils de navigation ou appelés à l'être. Les smartphones peuvent également être utilisés pour localiser des personnes.

Un employeur peut avoir un intérêt légitime à localiser ses collaborateurs et/ou leurs véhicules, par exemple pour planifier plus efficacement l'affectation de ses collaborateurs du service externe ou pour saisir un temps précis d'intervention auprès d'un client. Il importe toutefois que le collaborateur concerné soit entièrement informé des technologies employées ainsi que de ses intérêts et du but visé par le traitement des données ainsi collectées. Le traitement de ces données est autorisé dans la mesure où les principes de la légalité, de la finalité, de la proportionnalité, de la transparence et de la bonne foi sont respectés. L'employeur doit veiller à ce que le traitement se limite aux données qui sont effectivement pertinentes pour l'exécution du contrat de travail ou pour la réalisation des objectifs commerciaux. Dans ce contexte, il doit s'abstenir d'utiliser les possibilités techniques permettant de collecter d'autres informations, telles que l'itinéraire choisi ou la vitesse du véhicule d'entreprise.

Par ailleurs, la surveillance en temps réel et la surveillance en dehors des horaires de travail requièrent une justification particulière: une localisation en temps réel peut évoluer vers une surveillance du comportement à des fins de profilage, constituant une atteinte à la personnalité. Ce type de surveillance est également proscrit par le droit du travail dès lors que les objectifs de l'employeur peuvent être atteints par des moyens moins intrusifs.

Dans tous les cas, il n'existe aucune base légale autorisant la poursuite de la surveillance après la fin de la journée de travail d'un véhicule de fonction ou d'un téléphone mobile professionnel pouvant également être utilisés à titre privé. C'est pourquoi il convient de veiller à ce que l'employeur n'ait plus accès aux données de localisation après la fin de la journée de travail.

1.7.4 Saisie du temps de travail à l'aide des empreintes digitales dans la restauration

Les systèmes biométriques de saisie du temps de travail et de contrôle des accès sont de plus en plus utilisés dans le secteur de la restauration. Les données telles que les empreintes digitales étant qualifiées de particulièrement sensibles, leur utilisation doit être réfléchie et restrictive.

Les systèmes biométriques de saisie du temps de travail, de contrôle des accès ou de gestion des caisses sur lesquels les collaborateurs doivent s'identifier au moyen de leurs empreintes digitales sont très répandus, y compris dans la restauration. Parfois, la conclusion ou le maintien d'un contrat de travail est subordonné au consentement de l'employé pour l'enregistrement de ses empreintes digitales. Plusieurs personnes concernées ont contacté notre hotline à ce sujet au cours de l'année sous revue.

Les données biométriques telles que les empreintes digitales sont indissociables d'une personne et ne peuvent pas être simplement remplacées en cas de perte. C'est pourquoi des exigences de sécurité accrues s'appliquent dans le traitement de ces données sensibles. Elles ne peuvent notamment être traitées que si cela est nécessaire pour le but prévu. Afin d'empêcher l'accès de tiers non autorisé aux données biométriques des collaborateurs, leur stockage central sur un serveur est à proscrire: elles doivent être conservées exclusivement sur un support local, par exemple un badge, qui doit être lu en même temps que les empreintes. Pour le respect du principe de proportionnalité, il peut être utile de traiter uniquement un extrait des empreintes digitales, plutôt que les empreintes complètes.

Pour préserver le droit des collaborateurs à l'autodétermination, il paraît souhaitable de leur proposer des alternatives à la saisie biométrique du temps de travail. Quant à savoir si un employeur est autorisé à conditionner l'embauche d'un collaborateur à la saisie de ses empreintes digitales, cette question relève en premier lieu du droit du travail. Les employés qui souhaitent à titre individuel contester l'introduction de systèmes biométriques de saisie du temps de travail peuvent s'adresser à un tribunal des prud'hommes.

1.8 Économie et commerce

1.8.1 Privacy Shield entre la Suisse et les États-Unis

Au cours de l'année sous revue, nous avons accompagné la mise en place de l'accord Privacy Shield entre la Suisse et les États-Unis, et avons publié un guide à l'intention des citoyens.

Dans notre 24^e rapport d'activités 2016/2017 (chiffre 1.8.1), nous avons consacré un article à l'accord Privacy Shield entre la Suisse et les États-Unis. Depuis lors, plus de 1000 entreprises ont obtenu une certification. Au cours de l'année sous revue, nous avons participé à la révision de l'accord Privacy Shield entre l'Union européenne et les États-Unis en qualité d'observateurs et un guide pratique destiné aux citoyens (cf. www.leprepose.ch, Protection des données, Commerce et économie – Transmission à l'étranger – États-Unis). Au cours de l'année à venir, la mise en œuvre du Privacy Shield Suisse-États-Unis sera également soumise à un premier réexamen. Il doit avoir lieu à l'automne 2018, en même temps que la révision de l'accord Privacy Shield UE-États-Unis. À des fins de coordination et de préparation des deux contrôles, notre autorité se concerta avec les autorités de protection des données de l'Union européenne et de ses États membres. Les premiers échanges ont eu lieu en janvier 2018 à l'occasion d'une visite du Préposé à Bruxelles.

Par ailleurs, une procédure a été lancée pour le recrutement de cinq juges, qui seront convoqués au besoin pour constituer le tribunal arbitral prévu par l'accord Privacy Shield Suisse-États-Unis. Le Département du Commerce américain a publié les postes à pourvoir au premier trimestre 2018. L'accès à la procédure arbitrale devrait également être mis en place cette année.

1.8.2 Fuite de données chez EOS Suisse

D'importantes quantités de données auraient été dérobées à la société de recouvrement EOS Suisse SA. Nous avons ouvert une procédure d'établissement des faits concernant cette affaire.

Selon un article du quotidien allemand *Süddeutsche Zeitung* du 27 décembre 2017, la société de recouvrement EOS a été victime l'an passé d'une fuite de données impliquant la transmission de plusieurs gigaoctets de données sensibles de patients. Parmi les personnes concernées se trouveraient notamment des patients de médecins et dentistes suisses. EOS nous a informés de la fuite de données présumée peu avant la parution de l'article. Afin de clarifier les aspects relatifs à la protection des données, nous avons ouvert, en date du

28 décembre 2017, une procédure d'établissement des faits à l'encontre d'EOS Suisse.

Dans le cadre de nos prises de position concernant les informations publiées par le journal *Süddeutsche Zeitung*, nous avons rappelé que les membres du corps médical ne peuvent transmettre à des tiers que les données qui sont effectivement nécessaires à la facturation ou au recouvrement. En cas de transmission injustifiée de données médicales à des tiers, les professionnels de la santé sont passibles de sanctions pénales.

1.8.3 Révision de la loi sur le droit d'auteur

Lors de la révision de la loi sur le droit d'auteur (LDA), nos principales demandes ont été retenues: elles concernaient la poursuite en cas de violations du droit d'auteur commises sur Internet, et en particulier la suppression du droit d'accès à l'information dans les procédures civiles.

Un jugement rendu dans l'affaire Logistep (cf. 18^e Rapport 2010/2011, ch. 1.3.5, et ATF 136 II 508) a déclenché une discussion enflammée concernant le traitement de données personnelles dans le cadre de la poursuite des violations du droit d'auteur sur Internet. Nous avons récemment publié des recommandations de bonnes pratiques à ce sujet (cf. 19^e Rapport 2011/2012, ch. 1.3.7, et cf. 20^e Rapport 2012/2013, ch. 1.3.3). L'obligation du législateur de garantir la sécurité du droit était quant à elle incontestée.

Sur la base des propositions émises par le groupe de travail AGUR12, mandaté par la conseillère fédérale Simonetta Sommaruga, un projet de révision de la loi a été élaboré. Nous avons constaté avec satisfaction que nos recommandations de bonnes pratiques ont été explicitement reprises dans une disposition de ce projet.

En revanche, nous avons déploré l'introduction d'un droit d'accès à l'information dans les procédures civiles. Selon ces dispositions, le détenteur d'un droit d'auteur pourrait, afin de faire valoir ses prétentions dans une procédure civile (p. ex. une prétention en dommages-intérêts pour violation du droit d'auteur), accéder à des données permettant l'identification d'abonnés. Ces données sont certes collectées et sauvegardées sur la base de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), mais ce, uniquement à des fins de poursuite et de répression de graves infractions pénales. L'utilisation de ces données dans une procédure civile représenterait selon nous une modification abusive de la finalité, et sortirait du cadre étroit autorisant la conservation des données (cf. 23^e Rapport 2015/2016, ch. 1.8.4).

Le Conseil fédéral a retenu notre critique en supprimant du projet de loi le droit d'accès à l'information. Dans sa nouvelle version, le projet de modernisation du droit d'auteur est ainsi compatible avec la protection de la personnalité.

1.8.4 Publicité personnalisée dans les applications utilisant des données de localisation

L'entreprise publicitaire APG/SGA nous a demandé de nous prononcer, sous l'angle de la protection des données, sur une plateforme d'affichage de publicités personnalisées dans les applications. Nous avons pris position et proposé des mesures.

Au cours de l'année sous revue, nous avons conseillé l'entreprise publicitaire APG/SGA, qui projette de mettre en place une plateforme permettant le ciblage personnalisé d'utilisateurs de terminaux mobiles (smartphones) dans la publicité en ligne. À cette fin, l'entreprise analyse les données de localisation et le comportement de l'utilisateur dans certaines applications. Ceci permet d'afficher des publicités ciblées dans des applications de prestataires tiers (p.ex. applications d'actualité). Le lien entre les données collectées et l'utilisateur est établi par un identifiant publicitaire, attribué par le fabricant du terminal mobile dès que l'utilisateur se connecte au moyen de son smartphone.

Il s'est avéré que l'utilisation de cette plateforme impliquait le traitement de nombreux profils de déplacement et données de localisation, pour une durée en principe illimitée. Selon nous, l'identification des personnes concernées est dans bien des cas relativement aisée, même si l'on utilise un identifiant publicitaire, et non le nom de l'utilisateur. Le but de ce modèle commercial étant en définitive de toucher un individu donné, dans un contexte donné, avec une publicité ciblée individuellement, nous partons du principe que le projet qui nous a été présenté comprend le traitement de données à caractère personnel. Les utilisateurs doivent donc recevoir, lors de l'installation des applications des prestataires tiers, des informations exhaustives et transparentes au sujet du traitement de leurs données. Leur consentement explicite est également indispensable. De plus, les utilisateurs doivent avoir la possibilité de révoquer à tout moment le consentement qu'ils auraient précédemment donné pour le traitement des données sur la plateforme publicitaire.

La société APG/SGA a pris bonne note de nos recommandations et examine actuellement leur mise en œuvre.

1.8.5 Traitement de données chez Admeira

Au cours de l'année sous revue, un premier échange d'informations a eu lieu avec la régie publicitaire Admeira, qui a également permis de définir la collaboration dans le cadre de notre activité de conseil.

Au cours de l'année sous revue précédente, nous avons conseillé Swisscom concernant ses obligations d'information de la clientèle en relation avec ses nouvelles dispositions de protection des données. Ces dispositions réglementent notamment la transmission de données de clients de téléphonie fixe à Admeira, la régie publicitaire détenue par Ringier, la SSR et Swisscom, sous une forme ne permettant pas l'identification des personnes. Les personnes concernées peuvent s'opposer à la transmission de ces données à des fins publicitaires.

Admeira traite ces données en vue de proposer à Ringier, la SSR et Swisscom des offres publicitaires adaptées à différents groupes cibles. Au cours de l'année sous revue, nous avons mené un premier échange d'informations avec Admeira pour suivre le projet et donner des indications concernant la protection des données. Par ailleurs, nous sommes en contact avec toutes les entreprises impliquées, et les accompagnons dans le cadre de notre fonction de conseil. Il s'agit également de veiller à ce que les flux de données et leur analyse soient entièrement transparents pour les personnes concernées.

1.8.6 Lettre d'information concernant la carte client de Coop

Au cours de l'année sous revue, l'entreprise de commerce de détail Coop a envoyé des courriers à certains clients pour les informer de nouvelles conditions de participation relatives à la carte client. En raison de demandes de personnes concernées, nous avons procédé à un examen des faits.

Les conditions générales de vente (CGV) de la carte client de Coop (Supercard) prévoient depuis l'année 2012 le traitement de données sur les paniers d'achats à des fins de profilage des clients. L'analyse des paniers d'achats n'était effectuée que si le client avait fourni son consentement explicite en cochant une case. Malgré plusieurs mesures et actions de communication par divers canaux, Coop déplore que de nombreux clients n'aient pas encore réagi à cette annonce de modification des CGV. Au cours de l'année sous revue, les personnes concernées ont à nouveau été personnellement contactées par courrier et informées au sujet des nouvelles CGV. Certains destinataires de ce courrier se sont alors adressés à nous, pour nous faire part de leurs inquiétudes concernant l'analyse des paniers d'achats.

Nos investigations auprès de Coop ont révélé que ce courrier d'information expliquait clairement comment les clients pouvaient refuser l'analyse des paniers d'achats. Les clients peuvent continuer d'utiliser leur Supercard même sans analyse de leur comportement d'achat. Ainsi, les exigences légales en matière de transparence et de consentement sont respectées. L'information fournie par Coop à ses clients était donc correcte.

1.8.7 Droits d'accès et d'opposition auprès d'un commerçant d'adresses – Résultat de la procédure devant le Tribunal administratif fédéral

Un commerçant d'adresses ne répondait pas aux demandes d'accès et d'effacement, violant ainsi ses obligations en matière de protection des données. Des personnes concernées s'en sont plaintes auprès de notre autorité. Nous avons saisi le Tribunal administratif fédéral, qui a admis notre action.

En raison de nombreux signalements qui sont parvenus concernant le commerçant d'adresses Lucency AG, en relation avec l'exercice des droits d'accès et d'opposition, nous avons émis une recommandation en septembre 2014. Notre recommandation n'ayant pas été suivie d'effet, nous avons engagé une procédure par voie d'action auprès du Tribunal administratif fédéral (TAF) (voir notre 23^e rapport d'activités 2015/2016, ch. 1.8.6).

Par jugement du 12 avril 2017 (A-5225/2015), le Tribunal administratif fédéral a admis notre action et a notamment obligé la défenderesse à répondre aux demandes d'accès selon l'art. 8 de la loi sur la protection des données, y compris aux demandes pendantes, dans le délai légal de 30 jours. De plus, le Tribunal a ordonné à Lucency AG de bloquer ou de supprimer les données personnelles à la demande des personnes concernées, ou de démontrer l'existence d'un motif justificatif pour la poursuite du traitement de ces données, et d'informer les personnes concernées en conséquence. En cas de non-respect de ces obligations, les membres du conseil d'administration sont passibles d'une amende pour insoumission à une décision de l'autorité en vertu de l'article 292 du Code pénal suisse (CP).

Le jugement est à présent exécutoire. Si, après cette décision de justice, l'accès aux données n'était toujours pas accordé ou la confirmation du blocage des données toujours pas communiquée, une dénonciation pénale (fondée sur l'article 292 CP) peut être déposée à l'encontre des membres du conseil d'administration de Lucency AG.

1.8.8 Communication de données à des tiers par le site d'enchères ricardo.ch

La plateforme d'enchères en ligne ricardo.ch a modifié sa déclaration de confidentialité, afin de permettre l'échange de données au sein du groupe Tamedia, notamment pour la publicité personnalisée. Nous avons ouvert une procédure afin d'examiner si une telle communication des données repose sur le consentement valable des utilisateurs.

La plateforme suisse de commerce et d'enchères en ligne ricardo.ch a modifié en juillet 2017 sa déclaration de confidentialité, afin de permettre la communication des données à des tiers, à savoir à des entreprises du groupe Tamedia et d'autres sociétés affiliées. L'échange des données au sein du groupe doit permettre à la fois la prévention d'abus et la publicité personnalisée. Ricardo.ch a informé ses utilisateurs de la modification de ses conditions d'utilisation par le biais d'un courriel, tout en précisant qu'en cas de refus, le compte serait automatiquement fermé. Les personnes qui ne réagissent pas à ce courriel sont réputées avoir accepté les nouvelles conditions d'utilisation.

La communication de données à des tiers à des fins de publicité personnalisée requiert le consentement libre et éclairé des personnes concernées; le consentement doit être au surplus explicite s'agissant de données sensibles ou de profils de personnalité. Nous avons ouvert une procédure d'établissement des faits afin d'examiner en particulier si l'entreprise peut se fonder sur le consentement de ses utilisateurs, voire sur un autre motif justificatif. Elle a répondu à nos questions et nous a présenté ses traitements de données. Nous sommes en train d'évaluer ces informations afin d'apprécier juridiquement les faits.

1.8.9 Les questions admissibles dans les formulaires de demande de location

Les questions concernant la confession des candidats intéressés à la conclusion d'un contrat de bail ne sont pas admissibles dans les formulaires de demande de location, dans la mesure où elles représentent une atteinte non justifiée à la sphère privée. Nous avons prié les régies immobilières concernées d'adapter leurs formulaires en conséquence.

Selon un article paru dans la presse à propos d'un fait divers, un certain nombre de régies immobilières demanderaient aux candidats intéressés à la conclusion d'un contrat de bail des informations concernant la confession. Or, la collecte systématique de données concernant les croyances religieuses – considérées par la loi comme des

données sensibles – constitue une atteinte à la sphère privée qui n'est en principe pas justifiée par l'intérêt privé prépondérant du bailleur ni par un autre motif justificatif.

Nous avons analysé les formulaires de demande de location des plus grandes régies immobilières de Suisse afin de vérifier s'il s'agissait d'une pratique répandue. Nous avons d'abord pu constater que l'Association suisse des propriétaires fonciers ne prévoyait pas cette question dans ses formulaires-types. Sur une trentaine de questionnaires examinés, nous avons identifié trois régies qui requéraient cette donnée dans leurs formulaires standardisés; nous en avons conclu que la collecte de données sur la confession n'était pas une pratique courante. Nous avons écrit à ces régies afin d'attirer leur attention sur la situation légale et les avons priés d'adapter leurs formulaires en conséquence.

Par ailleurs, nous avons révisé nos explications concernant la collecte de données effectuée par les régies immobilières. (Cf. «Formulaires d'inscription relatifs à la location d'un appartement» sur notre site www.leprepose.ch – Protection des données – Habitat et transports).

1.8.10 Ordonnances pour la mise en œuvre du premier train de mesures de la Stratégie énergétique 2050

Au cours de la procédure de consultation des offices, nous avons pris position sur les aspects de protection des données des ordonnances relatives au premier train de mesures de la Stratégie énergétique 2050: la publication de données personnelles sur Internet et le traitement des données par des systèmes de mesure intelligents (smart meter).

Dans le cadre de la procédure de consultation sur les ordonnances relatives au premier train de mesures de la Stratégie énergétique 2050, nous nous sommes prononcés sur la publication de données personnelles et sur le traitement des données par des compteurs intelligents. Il s'agit de thèmes sur lesquels nous intervenons déjà depuis plusieurs années dans le domaine de l'approvisionnement énergétique (cf. également notre 24^e rapport d'activités 2016/2017, chiffre 1.8.3 avec autres renvois).

L'Office fédéral de l'énergie (OFEN) avait l'intention de publier sur Internet les données personnelles de tous les bénéficiaires de rétributions uniques et de rétributions à prix coûtant du courant injecté (RPC). L'objectif de cette mesure aurait été d'assurer la transparence concernant l'utilisation du supplément facturé aux consommateurs finaux. Au cours de notre évaluation des projets de loi, nous nous sommes également penchés sur la pertinence de cette publication de données personnelles. L'extension de la publication Internet à tous les bénéficiaires de rétributions uniques et de RPC aurait porté atteinte au droit à l'autodétermination informationnelle de 5000 personnes supplémentaires, qui ne représentent que 8 pour cent des rétributions totales, ce que nous avons jugé disproportionné. L'OFEN a tenu compte de nos préoccupations: il maintient sa pratique de publication, mais ne publie les données personnelles des exploitants de nouvelles installations de production d'électricité à partir d'énergies renouvelables qu'à partir d'une puissance d'installation de plus de 30 kVA.

Pour les autres dispositions prévues au niveau des ordonnances concernant la publication, il n'existait pas de dispositions légales formelles qui auraient conféré au Conseil fédéral la compétence d'édicter des dispositions d'exécution concernant la publication de données personnelles. L'OFEN prévoit de créer la disposition légale nécessaire, et ne procédera aux adaptations dans les ordonnances qu'une fois que cette disposition sera entrée en vigueur.

Concernant les dispositions d'exécution sur les systèmes de mesure intelligents (notamment les compteurs intelligents), une seule divergence demeurerait au sujet de la fréquence de consultation des données. Ce point est sensible du point de vue du droit de la protection des données, notamment parce que les personnes concernées ont le sentiment d'être constamment observées. L'OFEN a élaboré une disposition d'ordonnance concernant la fréquence de consultation, comme le lui avait demandé le PFPDT, mais avait dans un premier temps fixé l'intervalle à une durée de 15 minutes, très courte selon nous, laquelle pouvait même encore être réduite lorsque la sécurité et l'efficacité de l'exploitation du réseau l'exigeaient. Après notre intervention, l'OFEN a augmenté l'intervalle à 24 heures, ce qui représente encore selon nous une fréquence inutilement élevée. Bien que la fréquence de consultation que nous préconisons, à un intervalle de deux semaines, soit tout à fait compatible avec la réalisation des buts de traitement, nous ne sommes pas parvenus à imposer cette exigence, même devant le Conseil fédéral in corpore.

1.8.11 Arrêt Moneyhouse

Comme nous l'annoncions au chiffre 1.8.2 de notre 24^e rapport d'activités 2016/2017, le Tribunal administratif fédéral a admis une grande partie de nos requêtes dans un jugement du 18 avril 2017 (A-4232/2015). Cette décision en justice n'ayant pas été portée devant le Tribunal fédéral, elle est à présent entrée en force.

1.8.12 Centrale d'information de crédit

Au cours de l'année sous revue, nous avons ouvert une procédure d'établissement des faits auprès de la Centrale d'information de crédit (ZEK) après avoir reçu des signalements de problèmes en relation avec la protection des données. Notre examen est encore en cours.

La Centrale d'information de crédit (ZEK) compile des informations sur la solvabilité dans les affaires de crédit de personnes physiques et morales, et les met à disposition de ses membres, en particulier des banques, contre rémunération. Plusieurs questions de citoyens et articles dans les médias ont attiré notre attention sur divers problèmes en relation avec la protection des données auprès de la ZEK. Ces signalements faisaient état, par exemple, d'informations insuffisantes fournies à des personnes enregistrées dans la base de données concernant les données collectées, d'entrées erronées dans la base de données, ou encore d'une procédure de rectification inefficace. Pour enquêter sur ces allégations, nous avons engagé en mai 2017 une procédure d'établissement des faits, qui est toujours en cours.

1.9 Finances

1.9.1 Échange automatique de renseignements

La mise en œuvre des nouvelles normes pour la lutte internationale contre la fraude fiscale et l'évasion fiscale se poursuit. Au cours de l'année sous revue, nous avons pris position concernant divers projets du point de vue de la protection des données.

a) Échange automatique de renseignements sur les comptes financiers

Dans le domaine de l'échange automatique de renseignements (EAR) sur les comptes financiers nouvellement instauré, la Suisse a commencé en 2017 à collecter des données qui doivent être échangées pour la première fois en 2018. La mise en œuvre de l'échange automatique de données avec un État requiert une activation bilatérale spécifique. Cela peut se faire de deux façons: soit par la signature d'un accord bilatéral, soit sur la base du Multilateral Competent Authority Agreement (MCAA, accord multilatéral entre autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers). Par cette procédure d'activation, les États participants s'engagent à intégrer la «norme commune de déclaration et de diligence raisonnable» de l'OCDE (norme commune de déclaration ou Common Reporting Standard, CRS) dans leur droit national et à l'appliquer (cf. notre 24^e rapport d'activités 2016/2017, ch. 1.9.1a).

Introduction de l'échange automatique de renseignements avec plusieurs États supplémentaires

Quel que soit le type d'activation choisi pour l'EAR, l'arrêté fédéral ou le traité bilatéral est soumis à l'approbation de l'Assemblée fédérale. Cette dernière avait approuvé en 2016 la mise en place de l'EAR avec une première série d'États, notamment les pays de l'UE (cf. notre 24^e rapport d'activités 2016/2017, ch. 1.9.1 a). Pour le moment, la Suisse a mis en œuvre l'EAR avec 38 États et territoires au total depuis le 1er janvier 2017; un premier échange d'informations sur les comptes aura lieu en 2018.

En juin 2017, le Conseil fédéral a adopté le message sur l'introduction de l'EAR avec 41 États partenaires supplémentaires, avec lesquels le dispositif sera mis en place à partir de 2018 pour un premier échange de renseignements sur les comptes en 2019. Nous avons souligné le fait que, sur ces 41 États et territoires, plus de 30 ne disposent pas d'un niveau adéquat de protection des données au sens de l'art. 6, al. 1 LPD (notamment la

Chine, la Russie et l'Arabie saoudite); pour ces États, des garanties supplémentaires en matière de protection des données sont nécessaires en vertu de l'art. 6, al. 2 LPD. Au cours de l'année sous revue précédente, nous avons déjà clairement souligné que la notification du 4 mai 2017 concernant les exigences de la Suisse dans le domaine de la protection des données, fondée sur le Multilateral Competent Authority Agreement (MCAA), n'était pas suffisante pour garantir un niveau adéquat de protection des données (cf. notre 24^e rapport d'activités 2016/2017, ch. 1.9.1a).

En même temps que le message concernant l'introduction de l'EAR avec 41 États partenaires, le Conseil fédéral a présenté au Parlement un projet d'arrêté fédéral portant sur un mécanisme de contrôle permettant de garantir la mise en œuvre conforme à la norme de l'échange automatique de renseignements. Selon ce mécanisme, le Conseil fédéral est chargé d'examiner, dans la perspective du premier échange de renseignements qui aura lieu en septembre 2019, l'avancement de la mise en œuvre de l'EAR dans les États partenaires, pour vérifier en particulier que ces États remplissent les conditions préalables pour l'introduction de l'EAR à la date du premier échange. Bien que cet instrument ne règle pas le problème de l'absence de garanties de protection des données selon l'art. 6, al. 2 LPD, nous nous sommes prononcés en faveur d'un tel mécanisme lors d'auditions devant la Commission de l'économie et des redevances du Conseil national (CER-N) en août et septembre 2017. À cette occasion, nous avons soutenu la nécessité pour le Conseil fédéral non seulement d'informer les commissions parlementaires concernant les résultats de son examen, mais également de les consulter. Un droit de consultation a été intégré dans l'arrêté fédéral lors des délibérations parlementaires.

Renforcement de la protection juridique dans le cadre de l'échange automatique de renseignements

Dans une motion du 2 novembre 2017 (n° 17.3973), la Commission de l'économie et des redevances du Conseil des États a proposé qu'il soit explicitement prévu dans la loi fédérale sur l'échange international automatique de renseignements en matière fiscale (LEAR) qu'aucun échange de renseignements ne peut avoir lieu pour les cas où une violation de biens juridiques essentiels est vraisemblable. Dans le cadre de la consultation des offices, nous nous sommes prononcés en faveur de cette motion. Le Conseil des États, en tant que conseil prioritaire, a approuvé la motion le 5 décembre 2017, contre l'avis du Conseil fédéral.

b) Échange automatique des déclarations pays par pays

En complément de la stratégie du Conseil fédéral concernant l'EAR, il est prévu d'accroître la transparence en matière de fiscalité des entreprises et de réduire l'optimisation fiscale de groupes multinationaux par l'échange automatique des déclarations pays par pays (EDPP). Début 2016, la Suisse a signé l'accord multilatéral portant sur l'échange des déclarations pays par pays (accord EDPP), et la loi EDPP est entrée en vigueur le 1er décembre 2017 (concernant nos prises de position sur cette loi, cf. notre 24^e rapport d'activités 2016/2017, ch. 1.9.1a). La protection des données est concernée en l'espèce car, selon le droit en vigueur, toutes les informations contenues dans les déclarations pays par pays se rapportant à une personne morale donnée sont considérées comme des données personnelles au sens de la loi sur la protection des données (cela changera avec l'entrée en vigueur de la LPD révisée). Au cours de l'année 2017, nous nous sommes exprimés plusieurs fois dans le cadre de consultations des offices au sujet de la liste de pays pour l'activation de l'échange des déclarations pays par pays. Nous avons souligné le fait que cette liste contient des pays qui figurent sur la liste des pays présentant un niveau insuffisant de protection des données établie par le PFPDT; des garanties supplémentaires en matière de protection des données doivent donc être exigées en vertu de l'art. 6, al. 2 LPD pour garantir un niveau adéquat de protection des données lors de la transmission de données personnelles dans ces pays. Nos interventions n'ont cependant pas été prises en compte.

1.9.2 Établissement des faits auprès de l'Administration fédérale des contributions

Au cours de l'année sous revue, nous avons engagé une procédure d'établissement des faits auprès de l'Administration fédérale des contributions (AFC), au sujet de la transmission de données dans le cadre de l'assistance administrative en matière fiscale entre la Suisse et les États-Unis. Sur cette base, nous avons émis une recommandation, selon laquelle, dans le cadre de l'assistance administrative internationale en matière fiscale, les personnes dont le nom doit être transmis mais qui ne sont pas formellement visées par les demandes d'assistance doivent être informées au préalable par l'AFC. En novembre 2017, nous avons engagé une procédure d'établissement des faits concernant la transmission de données personnelles par l'AFC dans le cadre de l'assistance administrative en matière fiscale entre la Suisse et les États-Unis. Il s'agissait notamment d'établir si, et en vertu de quelles bases, l'AFC transmettait ouvertement, c'est-à-dire sans caviardage, aux autorités fiscales américaines le nom de personnes qui n'étaient pas formellement visées par des demandes d'assistance et, si c'était le cas, si le droit à l'information préalable était respecté.

Sur la base des faits établis, nous sommes arrivés en décembre 2017 à la conclusion qu'il revenait aux tribunaux d'établir au cas par cas si l'AFC était autorisée à transmettre ouvertement le nom d'un tiers non formellement concerné, en particulier du collaborateur d'une banque; l'assistance administrative en matière fiscale ne doit pas servir à dissimuler une assistance administrative en matière pénale dirigée contre des collaborateurs des banques. Nous avons émis une recommandation, selon laquelle, dans le cadre de l'assistance administrative internationale en matière fiscale, les personnes qui ne sont pas formellement visées par les demandes d'assistance et dont le nom doit être transmis ouvertement doivent être informées au préalable par l'AFC conformément à l'art. 14, al. 2 de la loi sur l'assistance administrative fiscale.

L'AFC a rejeté notre recommandation, et nous avons donc soumis l'affaire au DFF pour décision. Dans l'attente d'une prise de position de ce dernier, le PFPDT réserve sa décision de saisir le Tribunal administratif fédéral.

1.10 International

Une collaboration étroite avec les autorités de protection des données afin de renforcer la coopération est indispensable à l'heure où les lois sur la protection des données sont nationales mais que l'échange de données personnelles ne connaît pas de frontières.

L'effectivité de la protection des données passe aussi par la coopération des autorités de protection des données au niveau international et par le développement de normes internationales. Il faut en effet pouvoir donner des réponses concertées aux traitements de données transnationaux auxquels nous sommes de plus en plus confrontés et garantir aux individus les mêmes droits indépendamment de leur lieu de domicile. Il est aujourd'hui plus que jamais nécessaire de se concerter avec les autorités chargées de la protection des données et du respect de la vie privée afin de déterminer comment réagir sur le plan technique et réglementaire aux principaux défis qui se posent en matière de protection des données tels que le Big Data, l'Internet des objets, l'intelligence artificielle et la surveillance de masse.

Les contributions de notre autorité jouent un rôle important sur la scène internationale dans les discussions sur la protection des données et le respect de la vie privée lors de forums internationaux, notamment auprès du Conseil de l'Europe, de la Conférence européenne et de la Conférence internationale des commissaires à la protection des données, des instances de contrôle communes Schengen et Eurodac et de l'Association francophone des autorités de protection des données (AFAPDP) ainsi que de l'OCDE.

Conseil de l'Europe

Les travaux de modernisation de la Convention pour la protection des données des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) ne sont pas encore achevés. Le dossier est toujours en mains du Groupe de rapporteurs du Comité des Ministres. Une finalisation des travaux par l'adoption par le Comité des Ministres d'un protocole d'amendement ou d'une convention révisée devrait intervenir dans le courant du premier semestre 2018. La Convention 108 actuelle compte désormais 51 États parties avec l'adhésion de la Tunisie le 1er novembre 2017. L'Argentine, le Burkina Faso, le Maroc et le Mexique ont été invités à adhérer.

Le Comité consultatif de la Convention 108 (T-PD) a adopté les lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées. Ces lignes directrices sont une première étape en vue d'une réglementation plus spécifique du recours aux mégadonnées.

Elles définissent un cadre général devant permettre de concevoir des politiques et des mesures de nature à rendre effectifs les principes énoncés dans la Convention 108 dans le contexte des mégadonnées. Le T-PD poursuit ses travaux de révision de la recommandation R (97) 5 relative à la protection des données médicales et élabore un guide pratique concernant la protection des données dans le secteur de la police. Il prépare également des lignes directrices concernant la protection des données traitées dans le cadre de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) et des lignes directrices concernant la protection de la vie privée et les médias.

Conférence européenne des commissaires à la protection des données

La conférence européenne des commissaires à la protection des données s'est déroulée à Limassol (Chypre) les 27 et 28 avril 2017 à l'invitation de la commissaire chypriote à la protection des données. La conférence a été l'occasion de faire le point sur la mise en place des réformes européennes et notamment le règlement général de protection des données qui entrera en vigueur le 25 mai 2018 et qui dotera les 28 États membres de l'Union européenne d'une législation forte et uniforme. L'un des points centraux de cette réforme est le renforcement des pouvoirs des autorités de protection des données (APDs) et notamment le renforcement des instruments de coopération et de coordination entre APDs. Dans une résolution, la conférence a également relevé l'importance de finaliser au plus vite la modernisation de la Convention 108 qui sera un élément central dans l'appréciation de la Commission européenne du niveau d'adéquation des États tiers. La Convention modernisée permettra également de faciliter la coopération entre les Parties et la conférence européenne pourrait dans le futur jouer un rôle non négligeable dans la collaboration entre APDs. En ce sens, la conférence a décidé de mettre en place un groupe de travail, dont le PFPDT devrait faire partie, appelé à faire des propositions sur le fonctionnement et le rôle de la conférence dans le futur.

La conférence a également permis d'échanger sur les politiques de sensibilisation menées par les APDs, sur les questions de responsabilité, de mise en conformité et de transparence dans le cadre de l'informatique en nuage. Elle a également abordé les défis de la génomique pour la protection des droits et des libertés fondamentales. Les données génomiques soulèvent de nombreuses questions d'ordre juridique, éthique, politique, économique et technique qu'il convient d'approfondir. Nos cadres juridiques doivent également être adaptés à ces développements

importants. Ainsi, nous avons rappelé que le respect du principe de minimisation des données, les obligations de transparence et d'annonce des violations de données, les évaluations d'impact, les principes de la protection des données dès la conception et par défaut, ou la certification, sont indispensables dans un tel contexte. La technologie doit aussi être sollicitée pour permettre de faciliter le traitement des données génétiques tout en garantissant les droits des personnes concernées. Il s'agit de pouvoir contrôler l'accès aux données tout en facilitant leur ouverture et leur partage à des fins médicales. Nous avons ainsi mentionné des recherches prometteuses menées actuellement par l'École polytechnique de Lausanne (EPFL) en vue d'une technologie de chiffrement dit homomorphe. Ces chercheurs travaillent en outre sur des outils statistiques capables d'empêcher de retrouver l'identité d'un patient à partir d'un jeu de données génétiques en principe anonymisées.

Groupe de travail sur la protection des données et l'action humanitaire internationale

La 37^e Conférence internationale des commissaires à la protection des données et à la vie privée a adopté une résolution sur la protection des données et l'action humanitaire internationale. Afin d'analyser les exigences en matière de protection des données dans l'action humanitaire internationale et de coopérer avec les acteurs concernés, un groupe de travail, piloté par notre autorité, a été créé. Le travail a abouti à la publication d'un manuel.

La 37^e Conférence internationale des commissaires à la protection des données et à la vie privée (CICPDVP) a adopté à Amsterdam en octobre 2015 une résolution sur la protection des données et l'action humanitaire internationale. À travers cette résolution, la CICPDVP s'est engagée à créer un groupe de travail pour analyser les exigences en matière de protection des données dans l'action humanitaire internationale et coopérer avec les acteurs concernés dans ce domaine. La participation au groupe de travail est pilotée par un représentant de notre autorité. Le groupe de travail s'est fixé les objectifs principaux suivants: comprendre les traitements et les technologies utilisés par les acteurs humanitaires, analyser le droit applicable et identifier les points problématiques afin de pouvoir proposer des lignes directrices pour améliorer les pratiques déjà existantes. Tout au long de ces deux dernières années, le groupe a principalement poursuivi deux pistes de travail. Il a, d'une part, développé l'expertise des autorités de protection des données en matière de protection des données dans le domaine humanitaire à travers des recherches et des rencontres. D'autre part, il a travaillé avec les acteurs humanitaires internationaux, principalement dans le cadre du projet «Protection des données dans l'action humanitaire» du

Brussels Privacy Hub (BPH) et du Comité international de la Croix Rouge (CICR). L'objectif du projet est de faire le lien entre action humanitaire et les lois de protection des données, de comprendre les impacts de l'utilisation des technologies sur la protection des données dans le secteur humanitaire et de proposer des lignes directrices prenant en compte ces impacts. Ce projet correspond tout à fait à l'esprit de la résolution adoptée par la CICPDVP en octobre 2015 à Amsterdam. Dans ce cadre, des autorités, des organisations humanitaires et des experts se sont réunis au sein d'ateliers thématiques abordant les nouvelles technologies au service de l'action humanitaire et les impératifs de protection des données personnelles qui s'y rapportaient. Ces ateliers ont mis en lumière la nécessité d'identifier et de mettre à la disposition des professionnels de l'action humanitaire les bonnes pratiques en matière de protection des données personnelles. Dans le cadre de sa mission, le groupe de travail ad hoc a mené des séances de travail avec le CICR et le BPH, où a émergé l'idée de créer un outil pratique à l'usage des professionnels. Le manuel, publié en anglais en juillet 2017 sur le site du CICR, reprend les principes fondamentaux et les bases légales de la protection des données personnelles et consacre un chapitre à chacune des technologies exploitant des données personnelles utilisées dans le contexte de l'action humanitaire.

Groupe de travail européen sur le traitement de cas relevant de la protection des données

La 29^e réunion du groupe de travail européen sur le traitement de cas relevant de la protection des données («Case Handling Workshop»), s'est tenu à Manchester du 20 au 21 juin 2017. Le groupe de travail, constitué de représentants de 29 autorités nationales de protection des données, s'est concentré sur plusieurs sujets sensibles actuels. Cette année, le groupe s'est principalement concentré sur le Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la Directive européenne 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins pénales. Le groupe a ainsi notamment abordé la problématique de la mise en œuvre du Règlement général sur la protection des données et la manière dont il impactera les différents États. La discussion a également porté sur les nouveaux droits des personnes concernées, de la notification des violations de protection des données, du traitement des plaintes et des mécanismes de coopération. Sur ce dernier sujet, nous avons eu l'occasion de présenter les mécanismes de coopération des États tiers. Dans un deuxième temps, la discussion a porté sur la manière dont les autorités chargées de la protection des données peuvent développer des solutions efficaces et collaboratives face aux menaces et aux problèmes de protection des données.

Premier atelier du Global Privacy Enforcement Network (GPEN)

En juin 2017 s'est tenue à Manchester la première réunion de coordination annuelle du «Global Privacy Enforcement Network» (GPEN). Le GPEN a été créé pour promouvoir une collaboration transfrontalière entre les autorités de protection de la vie privée. Cet événement a réuni les autorités de 34 pays compétentes pour vérifier la conformité des traitements de données sur le plan national. Ce réseau informel de coopération, dont nous faisons partie, permet des échanges d'expérience et de méthodologie, et contribue à améliorer l'expertise et la capacité de réaction dans les dossiers à composantes internationales.

L'atelier a réuni plus de 70 délégués de 34 autorités mondiales, ainsi que des experts des domaines de la protection des consommateurs et des télécommunications. Le programme s'est focalisé sur toutes les étapes cruciales de cas relatifs à la protection des données et du respect de la vie privée. L'accent a en particulier été mis sur l'échange international de compétences et d'expériences pratiques.

Groupe de travail de l'OCDE sur la sécurité de l'information et la protection de la sphère privée

Le groupe de travail sur la sécurité de l'information et la protection de la sphère privée de l'Organisation de Coopération et de Développement Économiques (OCDE) a consacré ses travaux à diverses recommandations. Le groupe s'est penché sur la version révisée du projet de Recommandation de l'OCDE sur la gouvernance des données de santé, élaboré en étroite coopération avec le Comité de la santé et un groupe consultatif informel d'experts. Cette dernière contient notamment une liste des douze principales mesures recommandées pour maîtriser les grands enjeux de la gouvernance des données de santé, ainsi que le calendrier des consultations et les travaux réalisés à ce jour. Les délégués ont mis en évidence la nécessité d'apporter encore des modifications en vue de clarifier davantage la description de la «dé-identification».

Les délégués ont discuté une proposition en vue de la mise au point d'un instrument global destiné à promouvoir la cohérence entre les instruments juridiques de l'OCDE qui établissent un cadre favorisant l'accès aux données, ainsi que le couplage et la réutilisation des données. Les délégués ont examiné la proposition et confirmé la nécessité d'une meilleure compréhension des concepts-clés. Ils ont également reconnu les difficultés que posent actuellement les questions de gouvernance des données et la nécessité d'en débattre au niveau international. Ils ont aussi souligné l'importance de poursuivre le travail d'analyse, d'une part, des avantages économiques liés à une amélioration de l'accès aux données, ainsi que, d'autre part, des coûts ou de la perte d'avantages potentiels associés à une absence d'amélioration. Cette discussion a permis de mettre en évidence les risques liés à la collecte des données, qui ne se limitent pas aux risques d'atteinte à la vie privée, mais comprennent aussi un risque de réduction de la qualité des données.

Finalement, les délégués se sont concentrés sur la recommandation de 2012 relative à la protection des enfants sur internet qu'il convient d'actualiser au vu des évolutions intervenues dans les politiques de protection des enfants dans le cyberspace depuis 2012. Les délégués ont souligné l'évolution des divers risques auxquels sont exposés les enfants sur le web et la nécessité de mieux mesurer et de renforcer le niveau d'éducation et de sensibilisation des enfants, mais également de leurs parents. La collecte de données personnelles sur les enfants par l'intermédiaire des applications mobiles et le rôle de l'autorisation parentale ont aussi été mentionnés comme des sujets à approfondir. La question se pose de savoir dans quelle mesure l'anonymat peut être considéré comme un facteur de risque et si la gestion de l'identité numérique devrait par conséquent être intégrée aux travaux. Le processus proposé pour le premier réexamen de la Recommandation est approuvé.

Conférence internationale des commissaires à la protection des données

La 39^e Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC) s'est tenue à Hong Kong, du 25 au 29 septembre 2017, à l'invitation de l'autorité hongkongaise de protection des données. Elle a réuni quelque 800 participants qui ont débattu des enjeux actuels de la vie privée, notamment de l'impact des technologies et de l'importance de l'éducation au numérique. Durant la conférence, les commissaires ont admis cinq nouveaux membres des autorités nationales chargées de la protection des données, à savoir du Japon, du Monténégro, de l'Afrique du Sud, de la Turquie ainsi que de l'autorité belge de contrôle pour les systèmes d'information de la police. La Conférence compte à présent 119 membres. Lors de la première journée, les commissaires ont discuté des échanges d'informations entre les gouvernements en mettant particulièrement l'accent sur la meilleure manière de protéger les données sensibles, de prévenir la discrimination et de gérer les risques. Les enjeux du partage de l'information ont été explorés sous différents angles. Les experts ont également expliqué les processus de gestion des risques, l'analyse éthique visant à éviter la discrimination et les complexités du partage au sein du gouvernement ainsi qu'avec d'autres acteurs. À la fin de la première journée, les premiers Prix «vie privée et protection des données» de l'ICDPPC ont été attribués. Pendant la deuxième journée, le Rapporteur spécial des Nations Unies sur le droit à la vie privée, Joseph Cannataci, a présenté les progrès réalisés dans son mandat et ses objectifs pour l'année à venir. Après cette intervention, les groupes de travail en matière d'éducation au numérique, de développement de nouveaux indicateurs de la protection des données, d'action humanitaire, de télécommunications et de coopération en matière d'application des lois ont fourni une mise à jour sur leurs activités. Les commissaires ont consacré beaucoup de temps à discuter des questions internes concernant la composition, la taille et les objectifs de la Conférence. Des élections ont eu lieu pour désigner un nouveau comité et une nouvelle présidente: Isabelle Falque-Pierrotin (Présidente de la CNIL) succède à John Edwards (Commissaire néo-zélandais). Finalement, la Conférence a adopté trois résolutions : la première relative à la protection des données dans les véhicules automatisés et connectés, la seconde relative à la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique et la troisième en vue d'explorer les possibilités futures en matière de coopération transfrontière dans l'application des lois. La prochaine conférence internationale aura lieu à Bruxelles et sera organisée conjointement par le CEPD et la Bulgarie ; elle aura pour thème principal l'éthique numérique. La conférence internationale en 2019 aura lieu en Albanie.

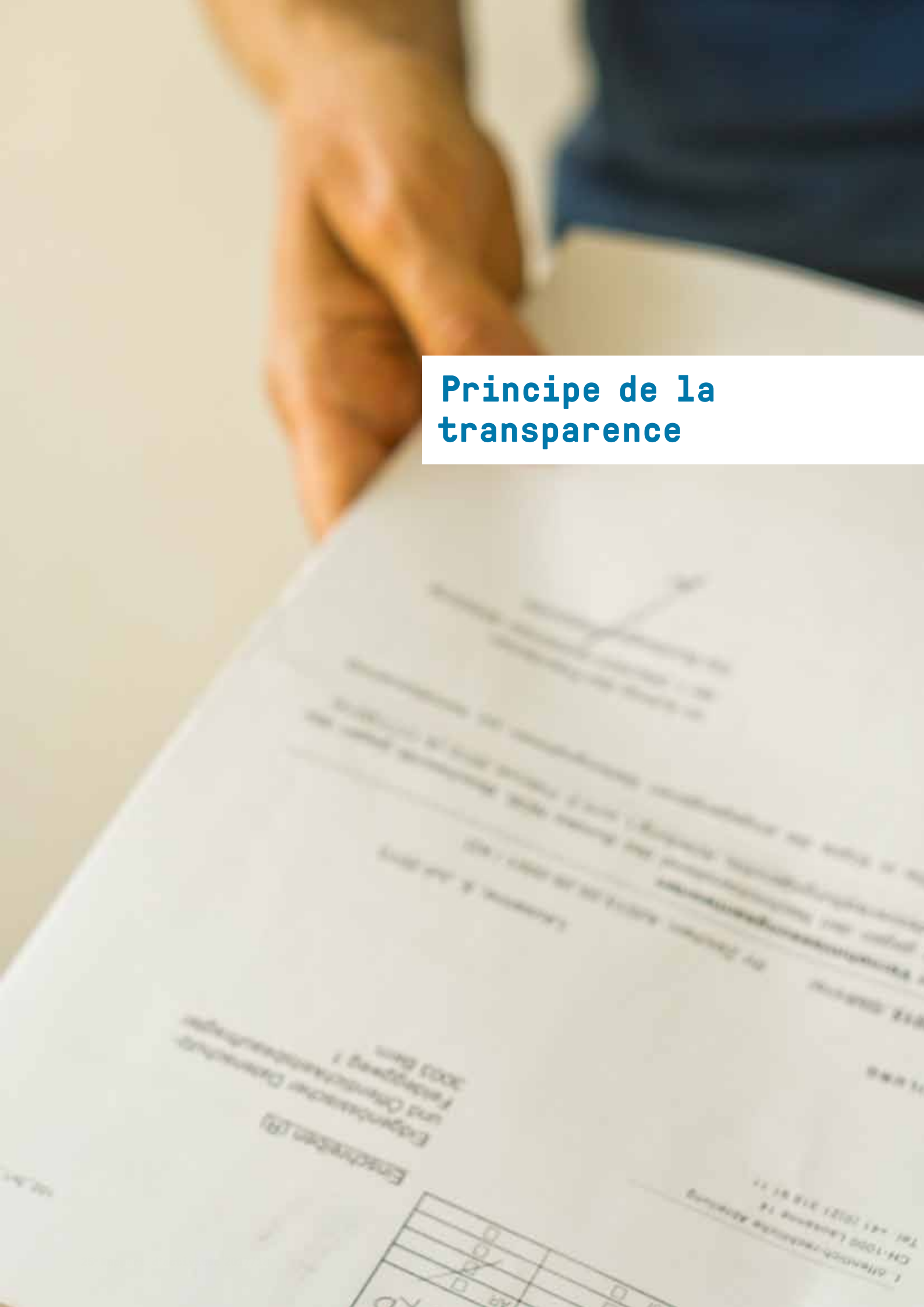
Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP), présidée par le Préposé suppléant, s'est réunie en conférence les 4 et 5 septembre 2017 à Gammarth, en Tunisie. À cette occasion, les participants ont débattu de la protection des données et l'action humanitaire internationale et discuté du manuel sur la protection des données dans l'action humanitaire internationale à la rédaction duquel l'AFAPDP a contribué (cf. ci-dessus). Les sujets de discussion ont porté sur la protection des données biométriques, le rôle du délégué à la protection des données et la portée extraterritoriale du Règlement général sur la protection des données.

Les membres de l'AFAPDP ont adopté une résolution qui porte sur l'accompagnement de l'intelligence artificielle par laquelle l'association attire l'attention sur le fait que les technologies d'intelligence artificielle doivent être au service des individus, dans le respect des droits et libertés individuels. L'AFAPDP attire l'attention sur le fait que le nécessaire accompagnement du développement des technologies d'intelligence artificielle et de l'innovation dans ce domaine doit se réaliser dans un esprit d'échange, de vigilance démocratique et de promotion des exigences garantissant le respect des droits et libertés des individus, dès la conception, notamment au regard de leur fiabilité, de leur intelligibilité et de leur sécurité vis-à-vis des individus, ainsi que de manière à garantir le droit de maîtrise de ces personnes sur les données qui les concernent. Elle souligne finalement la nécessité de soutenir l'adoption de législations relatives à la protection des données personnelles et à la vie privée dans l'espace francophone comme prérequis à un développement de ces technologies dans le respect des droits et libertés individuels.

L'AFAPDP a également proposé une formation aux techniques de contrôle aux agents des autorités membres. Elle a en outre célébré son dixième anniversaire au siège de l'Organisation internationale de la Francophonie à Paris, le 11 décembre 2017. Pour marquer cette occasion particulière, l'AFAPDP avait convié des écrivains francophones à venir partager leur vision de l'intimité, notion au cœur du travail des régulateurs. À l'issue des discussions, l'AFAPDP et l'Assemblée parlementaire de la Francophonie ont signé une convention de partenariat.

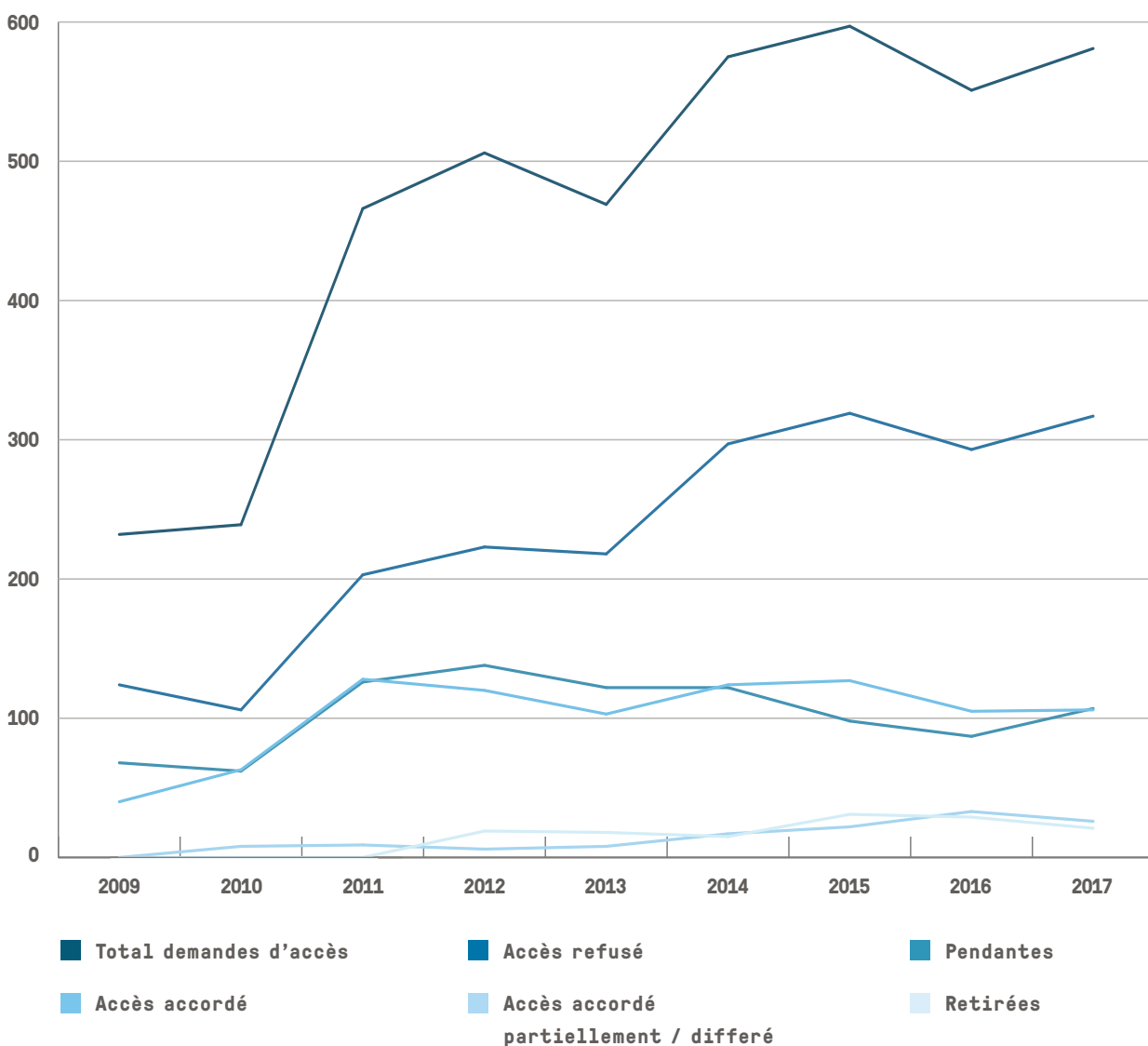
Principe de la transparence



2.1 Demandes d'accès

Selon les chiffres qui nous ont été communiqués pour l'année 2017, 581 demandes d'accès ont été soumises aux autorités fédérales (contre 551 en 2016). En 2017, le nombre de demandes d'accès s'est même élevé à 590 en incluant le Ministère public de la Confédération et les Services parlementaires (cf. 2.1.2 s.). Les autorités ont accordé un accès complet dans 317 cas (55%) (contre 293 en 2016 [53,17%]) alors que dans 106 cas (18%), les demandeurs n'ont reçu qu'un accès partiel aux documents (contre 105 en 2016 [19,05%]). Pour 107 cas (18%), l'accès a été entièrement refusé (contre 87 en 2016 [15,78%]). Par ailleurs, les autorités ont annoncé que 21 demandes d'accès (4%) ont été retirées (contre 29 en 2016 [5,26%]) et que 26 demandes (5%) étaient encore en suspens à la fin de l'année 2017 (contre 33 en 2016 [5,98%]).

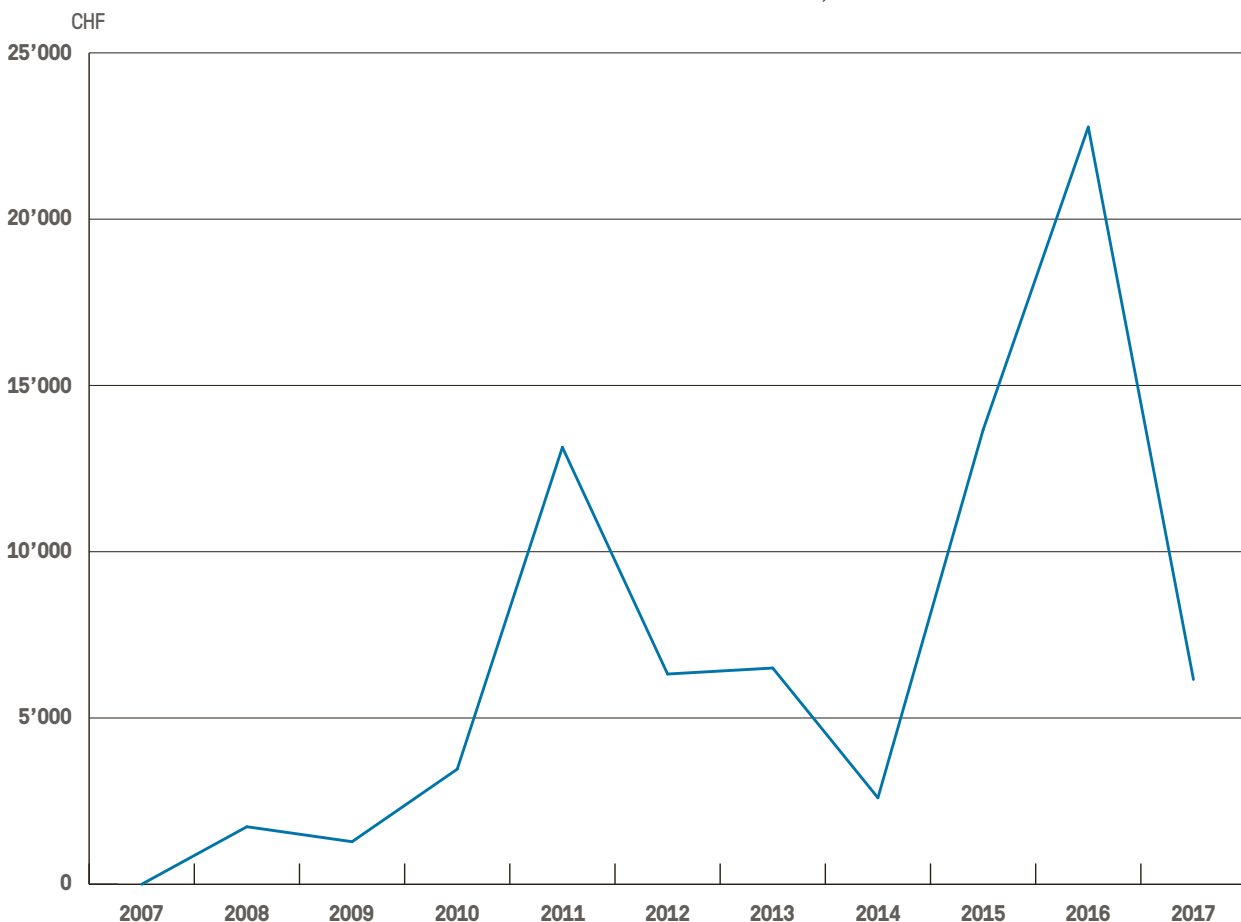
Globalement, le Préposé constate qu'après une forte augmentation du nombre de demandes d'accès entre 2013 (469 demandes) et 2014 (575 demandes), le nombre de demandes semble depuis s'être stabilisé pour se situer entre 550 et 600 demandes par année. En ce qui concerne le nombre total de demandes d'accès et la pratique des autorités y relative, les chiffres sont globalement stables par rapport aux années précédentes. Dans un peu plus de la moitié des cas, l'accès a été entièrement accordé, dans un cinquième des cas il a été partiellement refusé et, enfin, il a été entièrement refusé dans les cas restants. Depuis 2015, le Préposé constate par ailleurs une stabilisation du nombre de demandes faisant l'objet d'un accès complet à un peu plus de 50 pour cent. En comparaison, le nombre de demandes d'accès entièrement refusées a sensiblement diminué depuis 2015 pour se stabiliser aux alentours de 16,5 pour cent.



2.1.1 Départements et offices fédéraux

Au regard des chiffres qui ont été communiqués par les offices au Préposé, ce dernier constate que c'est l'OFSP qui a reçu le plus de demandes d'accès en 2017 (28), suivi de l'IFSN (23) et du SEM (21). Les départements ayant reçu le plus de demandes sont le DFAE (159), suivi du DEFR (81) et du DETEC (75). A l'opposé, 20 autorités nous ont communiqué n'avoir reçu aucune demande d'accès au cours de l'année 2017. Dans le même laps de temps, le Préposé a pour sa part reçu 13 demandes d'accès. Il a accordé entièrement l'accès dans 5 cas et partiellement dans 6 autres. Dans les cas restants, les documents officiels objets de la demande d'accès n'existaient pas.

Depuis l'entrée en vigueur de la loi sur la transparence, le Préposé relève que seules 130 demandes d'accès ont entraîné la perception d'un émolument, ce qui ne représente que 2,7 pour cent du total des demandes d'accès déposées auprès des Départements fédéraux et de la Chancellerie fédérale (4780). En comparaison, seuls 1,89 pour cent des demandes d'accès déposées en 2017 ont entraîné la perception d'un émolument (11 demandes sur 581). De ce fait, le Préposé constate que, comme lors des années précédentes, la gratuité est restée la règle et le paiement d'un émolument l'exception. Quant au total des émoluments perçus en 2017 pour l'accès à des documents officiels, celui-ci s'est élevé à 6160 francs. Il s'agit d'un montant largement moins élevé que celui perçu lors des deux années précédentes (2016: 22'770 fr.; 2015: 13'663 fr.). Il convient par ailleurs à nouveau de relever une certaine constance dans les différentes pratiques des autorités en matière d'émoluments. Alors que la Chancellerie fédérale et le DFAE n'ont à nouveau prélevé aucun émolument, les six autres départements ont partiellement facturé leur temps de travail aux demandeurs. Les émoluments facturés l'ont finalement été avec une certaine homogénéité (DFI: 1600 fr.; DFPJ: 200 fr.; DDPS: 1300 fr.; DFF : 1600 fr.; DEFR: 1300 fr.; DETEC: 160 fr.).



En ce qui concerne les heures de travail que représente le traitement des demandes, 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 effectivement effectuées pour le traitement des demandes. Selon ces données, le temps de travail annoncé cette année a diminué par rapport à l'année précédente (2017: 2968 heures; 2016: 3301 heures). Il reste toutefois plus élevé par-rapport à 2015 (2912 heures) et 2014 (1707 heures). En revanche, le temps de travail investi dans la préparation et la participation à des procédures de médiation a légèrement augmenté par-rapport à 2016 (2017: 914 heures; 2016: 857 heures), mais reste nettement inférieur aux chiffres de 2015 (1148 heures). Le temps de travail consacré à l'établissement d'une décision ou à une éventuelle procédure de recours n'a souvent pas été comptabilisé.

2.1.2 Services parlementaires

Les Services parlementaires nous ont annoncé avoir reçu 3 demandes d'accès en 2017. L'accès a été accordé dans les 3 cas.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a annoncé avoir reçu 6 demandes pour lesquelles l'accès a été accordé entièrement 5 fois et entièrement refusé dans le dernier.

2.2 Demandes en médiation

En 2017, 79 demandes en médiation ont été déposées auprès du Préposé, ce qui correspond à une diminution de 47 pour cent par rapport à 2016 (149). Tout comme l'année précédente, la plupart des demandes déposées l'ont été par des particuliers (99 sur 149 en 2016 et 35 sur 79 en 2017).

Ces chiffres permettent le constat suivant: dans 213 cas, l'Administration fédérale a refusé l'accès de manière totale (107) ou partielle (106). Ces données sont à mettre en perspective avec les 79 demandes en médiation qui sont parvenues au Préposé. Pendant l'année sous revue, seulement 37 pour cent des cas de demandes d'accès totalement ou partiellement refusées (77 % en 2016 et 43 % en 2015), ont fait l'objet d'une demande en médiation. 110 demandes en médiation ont malgré tout été réglées en 2017, parmi lesquelles 76 ont été soumises au cours de cette même année, 30 en 2016, trois en 2015 et une en 2014. Alors que pour les trois cas datant de 2015 les causes d'une telle durée de la procédure sont multiples (manque de coopération de l'autorité, prolongations des délais par les concernés, etc.), il s'agissait de suspendre la procédure en l'attente d'un jugement du Tribunal administratif fédéral pour celui de 2014.

En 2017, une solution consensuelle entre les participants a été trouvée dans 47 cas et le Préposé a émis 31 recommandations lorsqu'aucune solution amiable ne paraissait envisageable. Ces 31 recommandations ont permis de clore 40 cas. Par ailleurs, cinq demandes en médiation ont été retirées. Dans deux cas, les conditions d'application de la LTrans n'étaient pas remplies et dans quinze autres, la demande en médiation n'avait pas été soumise dans les délais. Enfin, une procédure en médiation déposée en 2017 a été suspendue conformément à la volonté des participants.

Toutes les recommandations émises pendant l'année sous revue sont disponibles sur le site internet du Préposé (www.leprepose.ch).

2.3 Procédure de médiation: évaluation de l'essai pilote mené en 2017

Afin d'accélérer la procédure de médiation et de réduire les cas pendants, nous avons mené en 2017 un essai pilote. Le rapport d'évaluation montre que cet essai a été un succès: les mesures prises ont permis d'atteindre les objectifs fixés. Au vu des résultats positifs, la nouvelle méthode sera intégrée dans la gestion ordinaire des procédures.

Comme nous l'annoncions dans notre dernier rapport d'activités, nous avons lancé en janvier 2017 un essai pilote portant sur une nouvelle méthode de traitement des procédures de médiation, destinée à raccourcir la durée des procédures et à réduire les cas pendants (cf. 24^e Rapport d'activités 2016/2017, ch. 2.4.1). Cette adaptation était justifiée par l'importance du nombre de nos recommandations et d'arrêts du Tribunal administratif fédéral et du Tribunal fédéral depuis l'entrée en vigueur de la loi sur la transparence

2.3.1 Essai pilote

Dans le cadre de l'essai pilote d'un an lancé le 1^{er} janvier 2017, les nouvelles demandes de médiation et, dans la limite du raisonnable, les demandes déjà pendantes ont été traitées majoritairement dans le cadre de médiations orales en présence des personnes et des autorités concernées. À défaut d'accord au cours de la séance de médiation, nous avons rendu oralement notre recommandation pendant l'essai pilote. La recommandation écrite, accompagnée d'une motivation sommaire, était adressée aux parties peu de temps après. Ce n'est qu'à titre exceptionnel qu'une recommandation écrite était directement émise, c'est-à-dire sans séance de médiation préalable, par exemple en présence de problématiques juridiques ou de cas de figure complexes, en cas de procédure collective (plusieurs tierces parties ou requérants impliqués) ou lorsque le dossier était limpide et la décision évidente (p. ex. non-entrée en matière).

Tableau 1: Durée de traitement des procédures de médiation

Durée de traitement en jours	Période 2014 à août 2016*	Phase pilote 2017
dans un délai de 30 jours	11 %	59 %
de 31 à 99 jours	45 %	37 %
plus de 100 jours	44 %	4 %

*Source: présentation du Préposé, manifestation pour les 10 ans de la LTrans, 2 septembre 2016.

Les trois objectifs fixés pour l'essai pilote étaient les suivants:

- respect des délais d'ordre dans au moins une partie des cas;
- augmentation de la proportion de solutions amiables;
- réduction à moyen terme des cas pendants.

Au début de l'année 2018, nous avons procédé à l'évaluation de l'essai pilote et présenté les résultats dans un rapport. Des extraits de ce rapport sont présentés ci-après. Le rapport d'évaluation complet est disponible sur notre site Internet (cf. www.leprepose.ch, Principe de la transparence – Évaluations).

2.3.2 Respect du délai d'ordre

Dans le tableau 1, les procédures de médiation ont premièrement été classées dans l'une des catégories suivantes en fonction du temps ayant été nécessaire à leur règlement: délai d'ordre légal de 30 jours respecté, durée de traitement de 31 à 99 jours, durée de traitement supérieure à 100 jours. La durée moyenne de traitement pour la période allant de 2014 à fin août 2016, ainsi que la durée de traitement des demandes en médiation reçues au cours de la phase pilote de l'année 2017, ont ensuite été intégrées sous la forme de pourcentages aux différentes catégories susmentionnées.

Entre 2014 et 2016, 11 pour cent des demandes déposées ont pu être traitées en respectant le délai d'ordre de 30 jours. Dans 45 pour cent des cas, la durée de traitement était comprise entre 31 et 99 jours et, dans 44 pour cent des cas, le traitement a pris plus de 100 jours. Au cours de la phase pilote, le délai d'ordre de 30 jours a pu être respecté pour 45 des 76 procédures de médiation, ce qui correspond à environ 60 pour cent des demandes réglées. Dans 28 cas (37 %), la durée de traitement se situait entre 31 et 99 jours et, dans seulement 3 cas (4 %), la procédure a duré plus de 100 jours.

Si l'on compare les pourcentages de l'année 2017 avec les valeurs moyennes de la période 2014–2016, on constate que le respect du délai d'ordre légal de 30 jours a progressé de manière significative au cours de l'essai pilote, passant de 11 à 59 pour cent. A l'opposé, le nombre de cas ayant nécessité un traitement de plus de 100 jours a été considérablement réduit, de 44 à 4 pour cent.

Conclusion: l'essai pilote a permis non seulement d'augmenter considérablement le nombre des demandes en médiation réglées dans les délais, mais également de réduire de façon conséquente, pour l'ensemble des procédures de médiation, le temps de traitement nécessaire.

Dans les cas restants, le dépassement du délai d'ordre de 30 jours était souvent dû à des raisons inhérentes aux cas eux-mêmes. Il s'agissait en particulier des raisons suivantes :

- report de la date de la séance de médiation sur demande des parties;
- cas de médiation nécessitant un surcroît important de travail;
- attente jusqu'à l'expiration du délai prévu pour le dépôt des demandes en médiation lorsque plusieurs demandeurs ou tiers sont concernés dans la même affaire;
- temps supplémentaire nécessaire pour tenter de parvenir à un accord ou en raison d'une suspension de la procédure en accord avec les parties;
- réception de nombreuses demandes en médiation dans un bref laps de temps.

En ce qui concerne la mise en œuvre de la procédure de médiation, il convient de noter que les courts délais d'ordre sont dans un rapport de tension avec la recherche d'accord dans le cadre de la procédure de médiation.

2.3.3 Proportion des solutions amiables

Pour répondre à la question de savoir si, en comparaison avec la période de 2006 à 2016, le projet pilote a permis d'augmenter la proportion de solutions amiables, le rapport entre le nombre d'accords et de recommandations a été calculé pour chacune des périodes. Trois périodes ont été analysées. La première concerne l'ensemble des résultats de l'activité de médiation des années 2006 à 2016. La deuxième, s'étendant de 2013 à 2016, a été choisie, car c'est à partir de 2013 que l'on a commencé à recourir de plus en plus fréquemment aux séances de médiation. Pour la troisième, soit celle de l'essai pilote, l'examen a porté non seulement sur les demandes reçues au cours de l'année 2017, mais également sur les 33 procédures de médiation encore pendantes cette année-là.

Tableau 2: Rapport entre recommandations et solutions amiables

Rapport entre recommandations et solutions amiables	
2006-2016	25 % de solutions amiables
2013-2016	40 % de solutions amiables
2017	60 % de solutions amiables

Au total, jusqu'en 2016, 25 pour cent des procédures ont été réglées par solution amiable. De 2013 à 2016, 40 pour cent des cas ont abouti à une solution amiable. En 2017, 60 pour cent des procédures de médiation ont été réglées par solution amiable, contre 40 pour cent par recommandation.

Conclusion: l'essai pilote a permis d'augmenter considérablement la proportion de solutions amiables.

2.3.4 Analyse des questionnaires de retour d'expérience

Depuis plusieurs années, à la fin de chaque séance de médiation, les participants sont invités à remplir un questionnaire de retour d'expérience. Pour chaque question, la personne interrogée peut attribuer un nombre de points allant de 5 (note la plus élevée) à 1 (note la plus basse).

Le rapport final d'évaluation contient également une analyse de ces questionnaires de retour d'expérience. Les avis des participants portant sur la période de l'essai pilote ont également été analysés. Le tableau 3 compare les résultats de l'essai pilote avec ceux de l'évaluation de 2014.

En 2017, sur les 80 questionnaires ayant été analysés (contre 52 lors de l'évaluation de 2014), 37 ont été remplis par les demandeurs (contre 25 en 2014) et 43 par les représentants des autorités fédérales (contre 27 en 2014). L'analyse de tous les questionnaires de retour d'expérience remis révèle que les résultats étaient et restent excellents. Selon le Préposé, les appréciations très favorables des participants démontrent également clairement l'importance et l'impact positif des séances de médiation dans le règlement amiable des demandes d'accès selon la loi sur la transparence, ce qui contribue également à une amélioration des relations entre l'administration et les citoyens.

Tableau 3: Analyse des questionnaires de retour d'expérience, moyenne arithmétique

Questions	Essai pilote 2017	Évaluation 2014
1. Je suis satisfait(e) du déroulement de la séance de médiation. (satisfait(e) - insatisfait(e))	4.3*	4.4*
2. Selon moi, la séance de médiation s'est déroulée dans un climat de confiance. (correct - incorrect)	4.7*	4.5*
3. J'ai le sentiment que la médiation a été menée de façon juste et équitable. (correct - incorrect)	4.7*	4.8*
4. J'ai le sentiment que les médiateurs ont entendu mes préoccupations, les ont prises au sérieux et ont tenté d'y répondre. (correct - incorrect)	4.7*	4.8*
5. J'ai le sentiment que la partie adverse a entendu mes préoccupations et a tenté d'y répondre. (correct - incorrect)	3.5*	3.8*
6. La salle de réunion m'a fait une impression (agréable - désagréable).	4.1*	3.9*
7. Globalement, j'ai une impression (positive - négative) de la séance de médiation - indépendamment du résultat.	4.5*	4.6*
Nombre de questionnaires de retour d'expérience évalués	80	52

* Le nombre maximum de points pouvant être attribués est de 5

2.3.5 Réduction du nombre de cas pendants

À la fin de l'année 2016, 33 procédures de médiation étaient pendantes. Sur les 79 demandes en médiation déposées en 2017, 76 avaient été réglées à la fin de l'année. Deux cas étaient encore en cours de traitement à ce moment-là et un cas avait été suspendu d'un commun accord entre les parties.

Le tableau 4 présente le nombre de procédures de médiation pendantes à la fin de l'année 2016 ainsi qu'à la fin de l'essai pilote.

Conclusion: à la fin de l'année 2017, le nombre de procédures de médiation pendantes avait été ramené de 33 à 3.

Tableau 4: Procédures de médiation pendantes

Procédures de médiation pendantes	
Fin 2016	33
Fin 2017	3 (2 cas en cours de traitement; 1 suspension)

2.3.6 Résumé

Globalement, le Préposé estime que les résultats de l'essai pilote mené pendant un an sont positifs. Les trois objectifs qu'il avait fixés ont été atteints:

- Pour les demandes en médiation déposées en 2017, le délai d'ordre de 30 jours a pu être respecté dans près de 60 pour cent des cas. Dans les cas où cela n'a pas été possible, le dépassement résultait de causes inhérentes aux cas eux-mêmes. Il convient par ailleurs de noter qu'il existe une tension entre le court délai d'ordre et le but de la procédure de médiation.
- La proportion de solutions amiables a pu être considérablement augmentée par rapport aux périodes antérieures. Un accord a été trouvé dans 60 pour cent des procédures de médiation traitées au cours de l'essai pilote.
- La quasi-totalité des cas pendants des années précédentes ont pu être traités.

Au vu des résultats positifs, le Préposé a décidé d'intégrer l'essai pilote dans la gestion ordinaire des procédures. Les mesures mises en œuvre avec succès (majorité de procédures orales, motivation sommaire des recommandations, procédures écrites uniquement à titre exceptionnel) seront intégralement conservées pour la mise en œuvre des procédures de médiation. Des adaptations aux évolutions et enseignements futurs restent bien entendu réservées.

2.4 Consultations des offices

2.4.1 Ordonnance sur le service de renseignement

Le projet d'ordonnance relative à la nouvelle loi sur le renseignement contenait dans sa première version une disposition qui aurait soustrait à la loi sur la transparence pratiquement tous les documents du Service de renseignement de la Confédération (SRC). Nous avons critiqué cette disposition, qui a été supprimée à l'issue de la consultation.

Selon la loi fédérale sur le renseignement (LRens) entrée en vigueur le 1^{er} septembre 2017, la loi sur la transparence (LTrans) ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations au sens de la LRens. Le projet d'ordonnance sur le service de renseignement (ORens) prévoyait dans sa première mouture une disposition d'exécution concernant cette exception prévue par la LRens. Dans le cadre de la première consultation des offices, nous nous sommes opposés à cette disposition, car elle ne limitait plus l'exception à la LTrans à la recherche d'informations par le Service de renseignement, protégée par des impératifs de droit supérieur, mais l'étendait de manière abusive à l'ensemble des documents et des informations détenus par le SRC. Les modifications que nous avons proposées n'avaient pas été prises en compte avant la procédure de consultation (cf. notre 24^e rapport d'activités 2016/2017, chiffre 2.3.3).

À l'issue de la procédure de consultation, le SRC a soumis à une nouvelle consultation des offices un projet modifié de l'ORens, qui ne contenait plus la disposition susmentionnée. Nous avons salué cette évolution. L'ordonnance sur le service de renseignement est entrée en vigueur le 1^{er} septembre 2017.

2.4.2 Arrêt du Tribunal fédéral: accès aux déclarations d'atteintes à la sécurité et d'incidents dans les transports publics

Le Tribunal fédéral a décidé que les atteintes à la sécurité et les incidents enregistrés dans une base de données détenue par l'Office fédéral des transports (OFT) devaient être rendus publics. Il a rejeté le recours de l'autorité qui souhaitait interdire l'accès à ces données à un journaliste.

L'Office fédéral des transports, compétent pour cette base de données, en avait refusé l'accès au motif qu'une publication de ces informations risquait de compromettre gravement son activité de surveillance. Il invoquait dans ce contexte la disposition d'exception prévue par la loi sur la transparence, selon laquelle l'accès à des documents peut être refusé lorsqu'il entrave l'exécution de mesures concrètes prises par une autorité conformément à ses objectifs. L'OFT craignait notamment qu'une divulgation ne dissuade les entreprises de transport de déclarer des incidents, avec un impact négatif sur la sécurité dans les transports publics.

Le Tribunal fédéral n'a pas retenu cette argumentation. Il a approuvé les considérants du jugement de l'instance inférieure, le Tribunal administratif fédéral, qui avait estimé que la disposition d'exception invoquée ne pouvait s'appliquer qu'à des mesures concrètes et ponctuelles d'une autorité, et non globalement à l'accomplissement des tâches et à l'activité de surveillance de cette autorité. Par ailleurs, comme l'a souligné le Tribunal fédéral, les entreprises de transport soumises à surveillance ont l'obligation légale de déclarer les événements menaçant la sécurité des transports, et on peut s'attendre à ce qu'elles la respectent. Dans le cas contraire, c'est ce comportement illicite des entreprises soumises à surveillance qui serait de nature à compromettre la prise de mesures adéquates par l'autorité de surveillance, et non la publication des informations disponibles en vertu de la loi sur la transparence. Selon le Tribunal fédéral, il incombe à l'OFT, dans le cadre de son activité de surveillance, de garantir par des contrôles et autres mesures adéquates le respect de l'obligation légale de déclaration des entreprises de transport et de sanctionner tout manquement éventuel. Le Tribunal fédéral a rappelé que le principe de transparence avait pour finalité de permettre un contrôle efficace des autorités publiques et de leur action (notamment de leur activité de surveillance). En l'espèce, ce contrôle n'est possible que si les informations rendues publiques précisent de quelles entreprises de transport, de combien et de quels types

d'incidents il s'agit, et sur quels trajets, ce qui est incompatible avec la préservation de l'anonymat des entreprises de transport. Le Tribunal fédéral a considéré qu'il existait un intérêt public prépondérant à la divulgation d'incidents dans les transports publics puisque ces entreprises, de par leurs rapports de concession et leur cofinancement par les pouvoirs publics, présentent une certaine proximité avec l'État (1C_428/2016 du 27 septembre 2017).

Comme l'affirme le Tribunal fédéral dans cet arrêt, le principe de transparence n'entrave pas l'activité de surveillance de l'OFT. Néanmoins, le 27 février 2018, dans le cadre de la discussion par article du projet d'organisation de l'infrastructure ferroviaire (OBI), le Conseil national s'est rangé à l'avis du Conseil fédéral en préconisant d'exclure de la loi sur la transparence l'activité de surveillance exercée par l'OFT en matière de sécurité (cf. notre 24^e rapport d'activités 2016/2017, ch.2.3.1).

2.4.3 Avant-projet d'ordonnance modifiant l'ordonnance sur l'accès aux documents du canton de Fribourg

Dans le cadre de sa collaboration avec les cantons, le Préposé a été invité par le canton de Fribourg à se prononcer sur l'avant-projet d'ordonnance modifiant l'ordonnance sur l'accès aux documents. Cette dernière, devant être adaptée à la Convention d'Aarhus, se fonde sur la loi du 5 octobre 2016 modifiant la loi sur l'information et l'accès aux documents (LInf-FR), sur laquelle le Préposé avait déjà été appelé à se prononcer en 2015 (cf. ch. 2.3.5 du 24^e rapport d'activités 2015/2016).

L'avant-projet d'ordonnance présenté au cours de l'année 2017 avait essentiellement pour but d'introduire les modifications nécessaires pour tenir compte de l'élargissement du champ d'application personnel et matériel de la LInf-FR, de prévoir de nouvelles normes procédurales, notamment en matière de délais afin de respecter les exigences de la Convention d'Aarhus, d'adapter les règles sur la compétence pour traiter de certaines demandes d'accès, ainsi que de supprimer, sur la base l'expérience acquise au cours des six premières années, différentes lourdeurs d'ordre procédural.

Dans sa prise de position, le Préposé s'est prononcé en faveur de l'avant-projet de révision proposé. Il a néanmoins tenu à rappeler que l'autorité ne doit pas pouvoir renoncer à la consultation au motif qu'une demande lui paraît d'emblée abusive. En effet, le principe de la transparence ne requérant pas du demandeur qu'il fasse valoir un intérêt digne de protection à pouvoir accéder à des documents ou qu'il justifie d'une utilisation particulière pour les obtenir, un éventuel comportement abusif du demandeur ne doit pas pouvoir être présumé trop facilement. L'autorité doit par conséquent examiner, dans chaque cas.



Le PFPDT

3.1 Tâches et ressources

Prestations et ressources dans le domaine de la protection des données

Effectifs

Depuis 2005, le nombre de collaborateurs affectés à l'application de la loi sur la protection des données (LPD) a fluctué entre 20 et 24. Ces fluctuations s'expliquent notamment par l'entrée en vigueur de la loi sur la transparence (LTrans) en 2006: comme les postes prévus pour ces nouvelles tâches n'ont jamais été validés par le Conseil fédéral, le PFPDT a dû y affecter des ressources existantes, et parfois également mobiliser les moyens de la Chancellerie fédérale. De plus, 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 pas pu être tous pourvus en raison de mesures d'économie. Dans son message concernant la révision totale de la LPD, le Conseil fédéral a laissé entrevoir au PFPDT la création de dix postes (FF 2017 6784). En raison du retard pris dans la révision totale (voir le chapitre 1.2.1 du présent rapport), on ne peut pas dire pour l'instant si les postes en question pourront être créés, ni, dans l'affirmative, quand ils pourront l'être.

Postes pouvant être affectés aux questions relatives à la LPD	2005	2010	2017	2018
	22	23	24	24

Conseil

Comme nous l'avons exposé au chapitre «Défis actuels et priorités», le PFPDT est confronté à une demande croissante et effrénée dans le domaine du conseil, en raison de la nécessité d'accompagner des projets de plus en plus grands et complexes. Durant la période sous revue, on a affecté pour la première fois plus de 50 pour cent des ressources aux prestations de conseil. La hausse des charges constituées par les conseils dispensés aux entreprises a été particulièrement marquée, passant de 18,2 à 20,8 pour cent. Selon la planification du PFPDT pour l'année 2018, l'accompagnement de treize grands projets est en cours.

Comme les ressources du PFPDT n'ont à ce jour pas été adaptées à l'augmentation des risques d'identification rétroactive et de détournements de données, ni aux autres

Conseil grands projets 2017	
Transport	3
Finances	2
Santé et travail	3
Sécurité	2
Télécommunication / Internet des objets	3

défis de la révolution numérique, le PFPDT n'est toujours pas en mesure de répondre à la demande accrue d'accompagnement de projets avec l'efficacité et le temps de travail requis. La hausse de la demande dans ce domaine l'oblige surtout à supprimer d'autres postes du groupe de prestations Conseil, par exemple au niveau de la collaboration internationale. Comme le big data et l'intelligence artificielle s'imposent comme modèles économiques dans des secteurs toujours plus nombreux, et que les risques technologiques pour la protection des données vont encore étendre le champ de la surveillance du PFPDT, le nombre de projets publics et privés impliquant un traitement des données va probablement continuer à croître, comme cela a été le cas au cours des années précédentes.

Prestations

Selon le Nouveau modèle de gestion de l'administration fédérale (NMG), les tâches du PFPDT – en tant qu'autorité de protection des données pour les organes fédéraux et l'économie privée – sont attribuées aux quatre groupes de prestations Conseil, Surveillance, Information et Législation. En 2016, les ressources humaines imputées au PFPDT pour la protection des données étaient réparties comme suit:

Conseil Entreprises	20.8 %	
Conseil Confédération	14.0 %	
Collaboration avec les cantons	4.6 %	
Collaboration internationale	11.9 %	
Total Conseils		51.3 %
Surveillance	10.8 %	
Certification	0.1 %	
Registre des données	1.3 %	
Total Surveillance		12.2 %
Information	13.5 %	
Formation/Conférences	4.4 %	
Total Information		17.9 %
Législation	18.6 %	
Total Législation		18.6 %
Total Protection des données		100.0 %

Surveillance

Actuellement, les contrôles doivent être effectués plus rapidement en raison de la dynamique des applications basées sur le cloud. Cette accélération ainsi que la nécessaire combinaison des connaissances juridiques et techniques excluent toute interruption longue dans les procédures d'établissement des faits, si bien que les contrôles de grande envergure doivent être suivis par plusieurs collaborateurs.

Les effectifs actuels restreignent considérablement la densité des contrôles. En 2016, environ 16 pour cent des ressources ont été affectées à l'activité de surveillance, ce qui est déjà bien inférieur à la moyenne à long terme de quelque 20 pour cent. Durant la période sous revue, ce chiffre a baissé une fois de plus de manière significative pour s'établir à 12 pour cent. Selon la planification pour l'année 2018, ces ressources devront servir à effectuer encore onze contrôles de grande envergure.

Si l'on compare ce chiffre aux quelque 12'000 grandes et moyennes entreprises que compte la Suisse, la densité des contrôles actuelle paraît faible. Le préposé aura de plus en plus de difficultés à faire part aux médias et aux organisations de protection des consommateurs de ses réticences à ouvrir formellement des procédures en vue de l'établissement des faits en raison des ressources limitées dont il dispose.

Législation

Le développement des nouvelles technologies, que le Conseil fédéral a qualifié de « fulgurant » dans l'introduction de son message concernant la révision totale de la LPD (FF 2017 6567), se répercute aussi sur le traitement des données par les organes fédéraux, qui n'est licite que s'il repose sur une base légale et qui se traduit dès lors par de très nombreuses prescriptions de traitement dans le droit fédéral, prescriptions sur lesquelles le PFPDT doit prendre position dans le cadre des diverses procédures de consultation. Le nombre des interventions dans ce domaine a fortement augmenté en dix ans, notamment durant la période sous revue, ce qui concourt aussi à la baisse de la densité des contrôles.

Révision totale de la LPD

Comme nous l'avons expliqué plus haut, les instruments de travail modernes comme les analyses d'impact relatives à la protection des données sont désormais utilisés dans le monde numérique. Ils sont en effet devenus affaire courante pour notre autorité dans le cadre du pilotage de grands projets numériques (voir le tableau ci-dessus). Pour consolider non seulement ces instruments de travail dans le respect de la sécurité du droit, mais aussi l'activité de surveillance du PFPDT qui en découle, il est indispensable que ces instruments soient inscrits aussi bien dans le RGPD que dans le droit suisse de la protection des données, comme le Conseil fédéral l'a prévu dans son projet de révision totale de la LPD. Étant donné que, en raison du retard pris dans la révision totale, on ne peut pas dire quand interviendra la création des dix postes dont il est question dans le message, notre autorité doit utiliser les nouveaux instruments de travail de manière pragmatique avec les ressources en personnel dont elle dispose.

Visite de service et auditions par les Commissions de gestion

Le 14 février 2018, la sous-commission DFJP/ChF de la Commission de gestion du Conseil des États – laquelle est responsable de l'unité PFPDT – a effectué une visite de service auprès de notre autorité. Durant cette visite, on a discuté, sur la base des chiffres du 24^e rapport d'activités 2016/17, de la charge de travail dans le domaine de la surveillance relevant de la protection des données, mais aussi de la baisse de la densité des contrôles qui en découlent. Par ailleurs, les auditions suivantes ont eu lieu: l'audition menée le 6 octobre 2017 par la sous-commission DFI/DETEC de la Commission de gestion du Conseil national au sujet des technologies numériques, du big data, de la billetterie électronique, de la technologie des capteurs et du style de vie dans la société numérique; l'audition menée le 20 mars 2018 par la sous-commission DFI/DETEC de la Commission de gestion du Conseil national au sujet de la cybersanté et du dossier électronique du patient; l'audition menée le 27 mars 2018 en séance plénière par la Commission de gestion du Conseil des États au sujet de la présentation et de la discussion concernant l'étude nationale sur la cyberadministration

Critères de quantification

La décision d'allouer ou non des ressources supplémentaires au PFPDT et la fixation de la date de cette allocation éventuelle relèvent de la responsabilité des autorités politiques, qui ont une marge d'appréciation considérable pour évaluer les évolutions actuelles et futures du monde numérique et leurs incidences sur l'activité de notre autorité.

La tâche principale du PFPDT consiste à protéger la sphère privée des particuliers et à garantir le droit à l'autodétermination informationnelle dans la société numérique. Le PFPDT doit pouvoir agir en toute indépendance. Cela requiert des ressources humaines, matérielles, techniques et financières adéquates et suffisantes, qui ne limitent pas l'autorité de surveillance à réagir simplement aux problèmes incontournables, mais qui lui laissent une réelle initiative dans l'action; cette action doit revêtir la crédibilité et l'intensité que les citoyens sont en droit d'attendre pour la protection de leurs droits fondamentaux.

En référence aux différents groupes de prestations, la quantification des ressources doit s'appuyer sur les objectifs suivants:

Groupes de prestations	Objectifs de résultats
Conseil	Le PFPDT déploie une présence conforme aux attentes pour le conseil aux particuliers et l'accompagnement de projets sensibles en matière de protection des données de l'économie et des autorités fédérales, en recourant à des instruments de travail adaptés à la sphère numérique.
Surveillance	Le PFPDT déploie une densité de contrôle crédible.
Information	Le PFPDT sensibilise le grand public de façon proactive aux risques liés aux technologies et aux applications dans le contexte de la numérisation.
Législation	Le PFPDT intervient activement, en amont, dans l'élaboration de toutes les normes spéciales et de tous les règlements ayant un impact en matière de protection des données, au niveau national et international. Il appuie les cercles intéressés dans la formulation de règles de bonne pratique.

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

Dans l'unité LTrans, à laquelle sont affectés 3,6 postes, des retards considérables se sont accumulés ces dernières années dans les procédures de médiation. Pour ne pas accroître encore ces retards et les résorber à moyen terme, le PFPDT a adopté depuis le 1er janvier 2017 une procédure sommaire et accélérée, caractérisée par la généralisation des médiations orales.

Comme le montre l'évaluation figurant au chapitre 2.3, cet objectif a pu être atteint, d'autant plus que le nombre de nouvelles demandes de médiation est resté stable si l'on compare les chiffres sur plusieurs années.

3.2 Publications au cours de l'année sous revue

Le site Internet www.leprepose.ch est le principal canal d'information du PFPDT. Il est régulièrement mis à jour et complété. L'ensemble des recommandations et des arrêts rendus dans le domaine de la loi sur la transparence y sont publiés. Dans le domaine de la protection des données, nous avons publié au cours de l'année sous revue deux guides détaillés à l'intention des entreprises suisses: un guide relatif au Privacy Shield Suisse-États-Unis, et un autre concernant le règlement général de l'UE sur la protection des données, entré en vigueur fin mai. De plus, le matériel d'enseignement pour les degrés secondaires I et II a été mis à jour.

Le règlement général de l'UE sur la protection des données (RGPD) est directement applicable aux entreprises suisses qui traitent des données de citoyens de l'UE ou qui offrent des services dans l'UE. Nous avons donc élaboré un guide contenant des informations tant sur les nouvelles obligations des entreprises que sur les droits des particuliers à la protection de leur sphère privée. Le RGPD renforce le contrôle dont disposent les citoyens sur leurs données personnelles (www.leprepose.ch, Documentation – Bases légales – Protection des données – International).

Depuis le 12 avril 2017, les entreprises américaines peuvent demander une certification pour adhérer au Swiss-US Privacy Shield et garantir ainsi un niveau de protection des données adéquat. Le PFPDT a publié une brochure intitulée «Guide relatif au Swiss-US Privacy Shield», qui contient des informations sur les obligations des entreprises certifiées et les droits des personnes concernées, ainsi que sur la procédure à suivre pour introduire une réclamation (www.leprepose.ch, Protection des données – Commerce et économie – Transmission à l'étranger – États-Unis).

Les personnes à la recherche d'un appartement à louer doivent souvent remplir des formulaires d'inscription dans lesquels elles transmettent de nombreuses informations personnelles. Nous avons publié des explications exposant en détail les informations qui peuvent légitimement être demandées sur ces formulaires et les questions qui ne sont pas admissibles au regard du droit de la protection des données (www.leprepose.ch, Protection des données – Habiter et transport – Formulaires d'inscription pour la location).

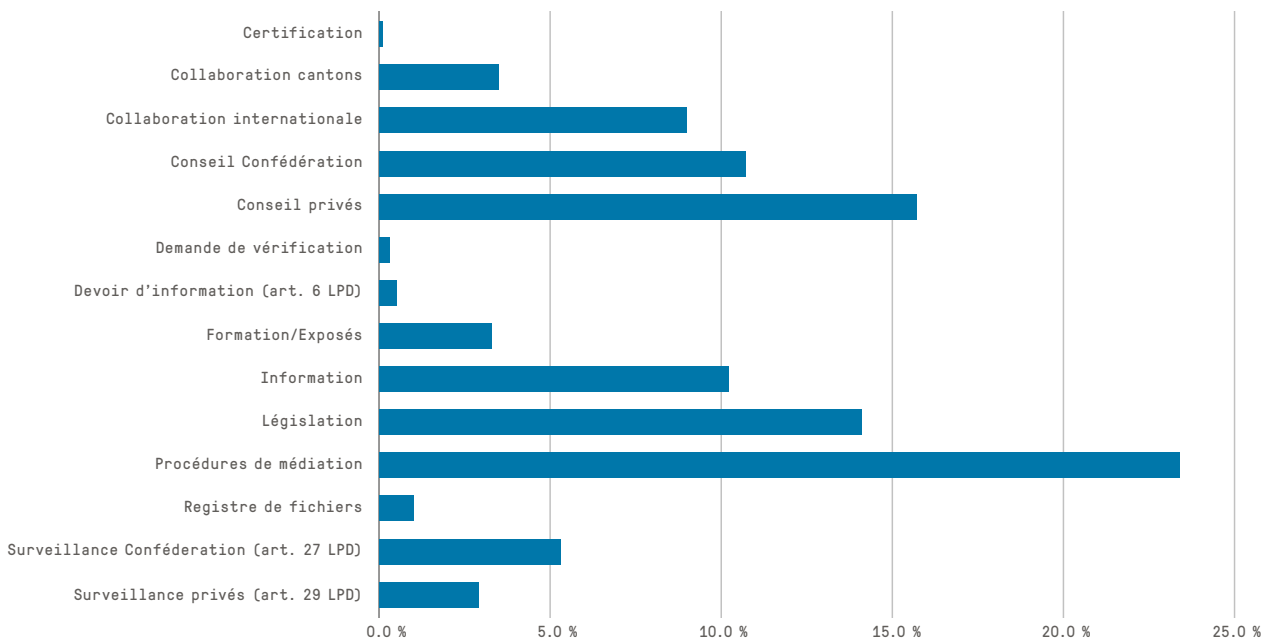
Pour qu'un employeur puisse transmettre à l'assurance d'indemnités journalières en cas de maladie les données dont elle a besoin, il doit disposer d'une procuration du collaborateur concerné. Les assureurs disposent d'une grande latitude dans la formulation de ces procurations. Cependant, ils sont tenus au respect du principe de la proportionnalité et doivent se limiter aux informations qui sont nécessaires au traitement du cas concrètement visé (www.leprepose.ch, Protection des données – Assurances – Assurance-maladie/accidents – Assurances d'indemnités journalières en cas de maladie).

Les unités didactiques sur la protection des données ont été remaniées l'an dernier. Toutes les leçons destinées aux élèves des degrés secondaires I et II sont à présent disponibles dans les trois langues nationales (www.leprepose.ch, Protection des données – Internet et ordinateur – Enfants et adolescents).

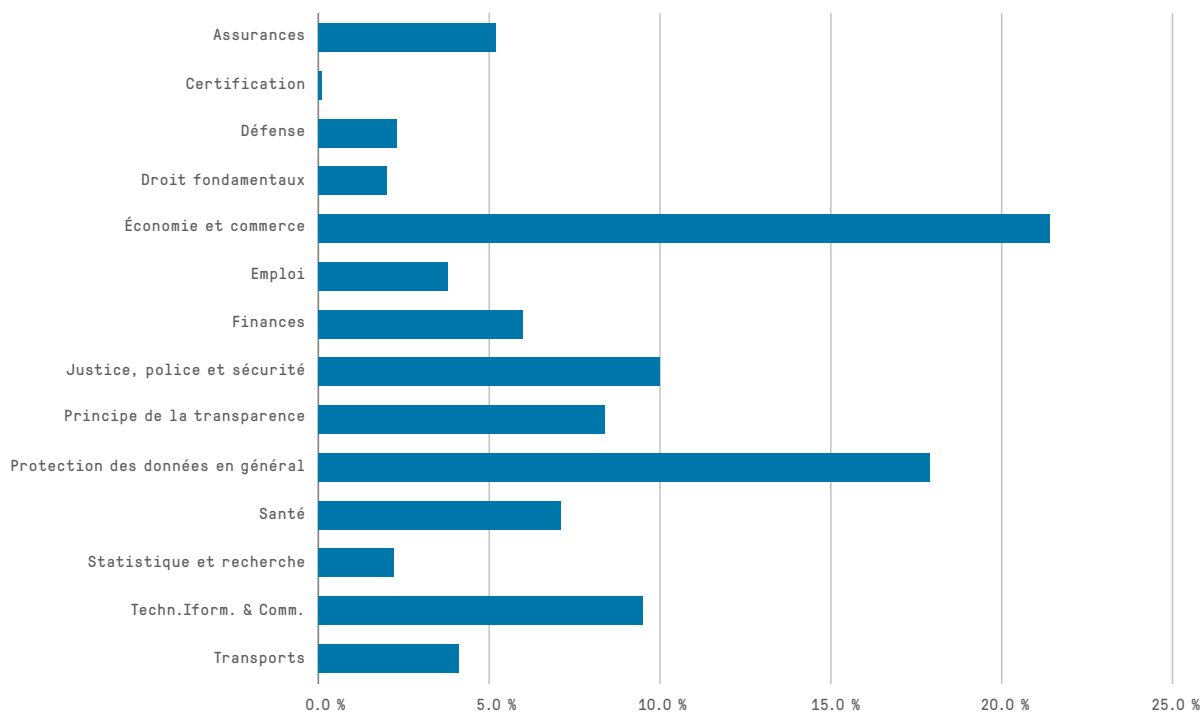
3.3 Statistiques

3.3.1 Statistiques des activités du PFPDT du 1^{er} avril 2017 au 31 mars 2018 (Protection des données et Principe de la transparence)

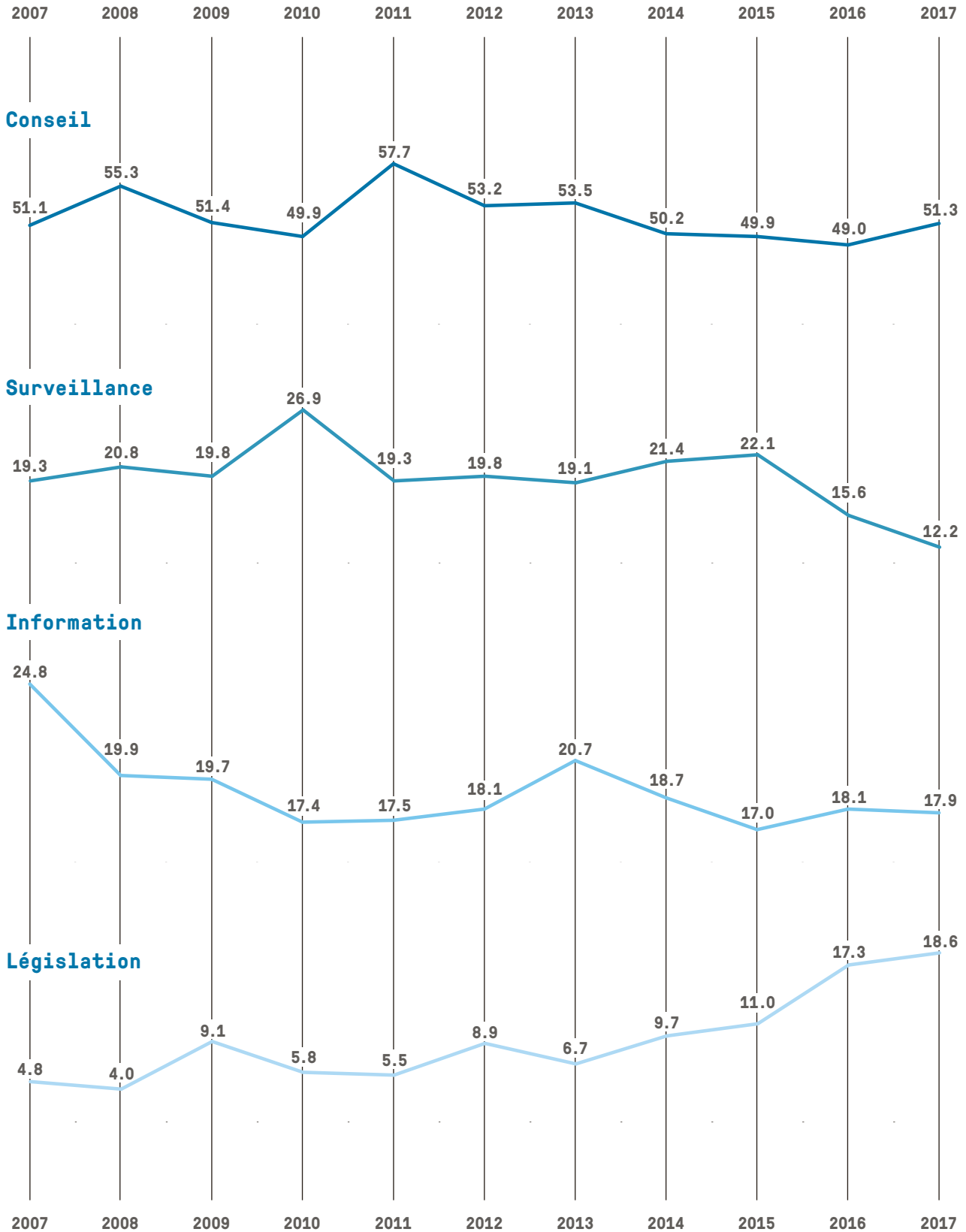
Charge de travail par tâches



Charge de travail par domaines



Comparaison pluriannuelle
(tous les chiffres en pourcentage)



3.3.2 Statistique des demandes d'accès selon la loi sur la transparence du 1^{er} janvier 2017 au 31 décembre 2017

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
ChF	17	10	6	0	1	0
PPPDT	13	5	0	6	0	0
TOTAL	30	15	6	6	1	0

Département fédéral des affaires étrangères DFAE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
DFAE	159	133	16	7	2	1
TOTAL	159	133	16	7	2	1

Département fédéral de l'intérieur DFI

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	0	0	0	0	0	0
BFEG	3	2	0	1	0	0
OFC	2	1	1	0	0	0
AFS	5	5	0	0	0	0
MétéoSuisse	0	0	0	0	0	0
BN	0	0	0	0	0	0
OFSP	28	9	3	8	5	3
OFS	1	0	0	1	0	0
OFAS	8	4	3	0	0	0
OSAV	10	6	1	2	1	0
MNS	0	0	0	0	0	0
SWISSMEDIC	11	2	2	4	0	3
SUVA	1	0	1	0	0	0
TOTAL	69	29	11	16	6	6

Département fédéral des finances DFF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	11	4	1	6	0	0
UPIC	3	1	0	2	0	0
AFF	4	2	1	1	0	0
OFPER	4	3	0	1	0	0
AFC	6	1	3	1	1	0
AFD	12	4	6	2	0	0
RFA	1	1	0	0	0	0
OFCL	9	5	0	3	0	1
OFIT	0	0	0	0	0	0
CDF	12	4	5	3	0	0
SFI	3	1	1	0	0	1
PUBLICA	0	0	0	0	0	0
CdC	4	1	1	2	0	0
TOTAL	69	27	18	21	1	2

Département fédéral de justice et police DFJP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	2	2	0	0	0	0
OFJ	4	2	1	0	1	0
FEDPOL	8	6	2	0	0	0
METAS	4	4	0	0	0	0
SEM	21	10	1	6	0	4
Service SCPT	1	0	0	1	0	0
ISDC	3	3	0	0	0	0
IPI	0	0	0	0	0	0
CFMJ	0	0	0	0	0	0
CAF	0	0	0	0	0	0
ASR	2	0	2	0	0	0
CSI	0	0	0	0	0	0
CNPT	0	0	0	0	0	0
TOTAL	45	27	6	7	1	4

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	0	0	0	0	0	0
OFT	5	3	0	0	0	2
OFAC	6	4	2	0	0	0
OFEN	12	6	0	2	2	2
OFROU	7	5	2	0	0	0
OFCOM	4	2	2	0	0	0
OFEV	14	9	2	2	1	0
ARE	0	0	0	0	0	0
ComCom	1	1	0	0	0	0
IFSN	23	5	3	4	9	1
PostCom	2	2	0	0	0	0
AIEP	1	1	0	0	0	0
TOTAL	75	38	11	8	12	5

Département fédéral de la défense, de la protection de la population et des sports DDPS

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	13	3	0	10	0	0
Défense/armée	6	3	1	1	1	0
SRC	10	3	7	0	0	0
armasuisse	16	1	11	4	0	0
OFSPD	8	7	1	0	0	0
OFPP	0	0	0	0	0	0
swisstopo	0	0	0	0	0	0
TOTAL	53	17	20	15	1	0

Département fédéral de l'économie, de la formation et de la recherche DEFR

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SG	17	6	1	10	0	0
SECO	20	10	5	4	0	1
SEFRI	8	4	3	1	0	0
OFAG	14	2	6	5	1	0
OFAE	4	2	2	0	0	0
OFL	0	0	0	0	0	0
SPr	1	1	0	0	0	0
COMCO	9	4	2	2	0	1
ZIVI	0	0	0	0	0	0
BFC	2	2	0	0	0	0
FNS	0	0	0	0	0	0
IFFP	0	0	0	0	0	0
CTI	0	0	0	0	0	0
Conseil des EPF	6	0	2	4	0	0
TOTAL	81	31	21	26	1	2

Ministère public de la Confédération MPC

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
MPC	6	5	1	0	0	0
TOTAL	6	5	1	0	0	0

Services du Parlement SP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
SP	3	3	0	0	0	0
TOTAL	3	3	0	0	0	0

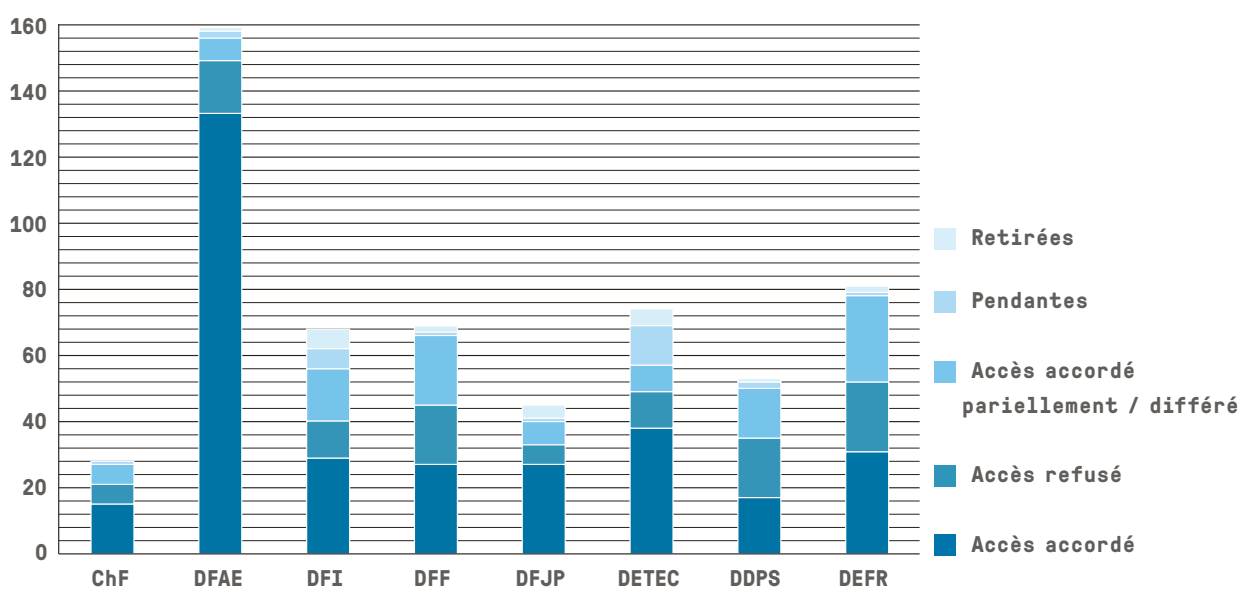
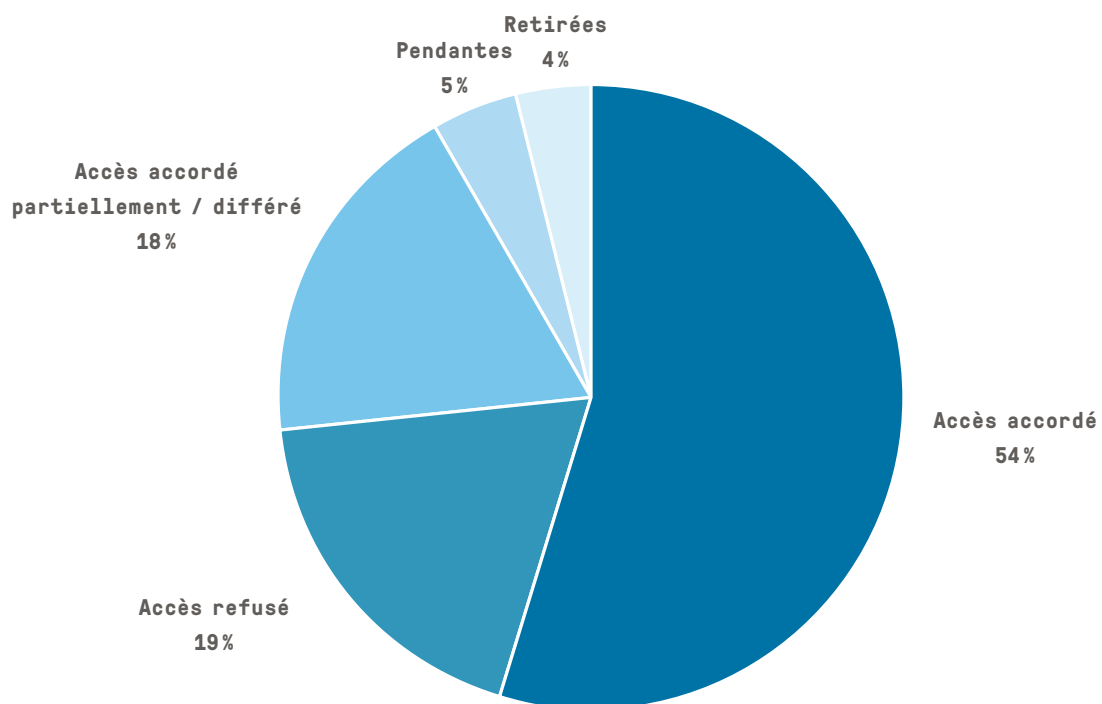
Vue d'ensemble des demandes d'accès de tous les départements et de la Chancellerie fédérale

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demandes d'accès pendantes	Demandes d'accès retirées
ChF	30	15	6	6	1	0
DFAE	159	133	16	7	2	1
DFI	69	29	11	16	6	6
DFF	69	27	18	21	1	2
DFJP	45	27	6	7	1	4
DETEC	75	38	11	8	12	5
DDPS	53	17	18	15	2	1
DEFR	81	31	21	26	1	2
TOTAL 2017 (%)	581 (100)	317 (55)	107 (18)	106 (18)	26 (5)	21 (4)
TOTAL 2016 (%)	551 (100)	293 (55)	87 (16)	105 (19)	33 (6)	29 (4)
TOTAL 2015 (%)	597 (100)	319 (54)	98 (16)	127 (21)	22 (4)	31 (5)
TOTAL 2014 (%)	575 (100)	297 (51)	122 (21)	124 (22)	17 (3)	15 (3)
TOTAL 2013 (%)	469 (100)	218 (46)	122 (26)	103 (22)	8 (2)	18 (4)
TOTAL 2012 (%)	506 (100)	223 (44)	138 (27)	120 (24)	6 (1)	19 (4)
TOTAL 2011 (%)	466 (100)	203 (44)	126 (27)	128 (27)	9 (2)	-
TOTAL 2010 (%)	239 (100)	106 (45)	62 (26)	63 (26)	8 (3)	-
TOTAL 2009 (%)	232 (100)	124 (54)	68 (29)	40 (17)	-	-

Nombre de demandes en médiation

Catégorie de requérants	2017
Médias	21
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	35
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	14
Avocats	2
Entreprises	7
Total	79

Traitement des demandes d'accès



3.4 Le Secrétariat du PFPDT

Préposé fédéral à la protection des données et à la transparence

Lobsiger Adrian
Suppléant: Walter Jean-Philippe

Domaine de direction Protection des données

Chef: Buntschu Marc

Suppléante: Haag Sophie

Team 1 Chef: Meier Thomas, juriste
Berger Cyrill, juriste
Frey Franziska, juriste
Weber Nathalie, juriste

Team 2 Cheffe: Gloor Scheidegger Caroline, juriste
Schönbett Frédéric, juriste
Trolliet Sabine, juriste

Team 3 Cheffe: Haag Sophie, juriste
Gisin Philipp, juriste
Krüsi Melanie, juriste
Rossier Odile, juriste

Domaine de direction Principe de la transparence

Team Chef: Ammann Reto
Keller Annina, juriste
Bulliard Florian, juriste (stagiaire)
Prinz Alessandra, juriste
Schwegler Astrid, juriste

Domaine de direction Centres de compétences

Chef: Tsiraktopoulos Kosmas

Suppléant: Sidler Andreas

Centre de compétence gestion des affaires, du personnel, des finances et de la communication

Secteur Gestion des affaires

Responsable: Jörg Paul

Fasel Frédéric, spécialiste technique I des services
administratifs et commerciaux

von Gunten Fabien, spécialiste technique I des services
administratifs et commerciaux

Secteur Communication

Meier Francis, délégué d'information

Böhlen Silvia, spécialiste en communication

Centre de compétence IT et Société

Chef: Sidler Andreas, informaticien/juriste

Aad Imad, informaticien

Däppen Daniel, informaticien

Scherrer Urs, informaticien

Domaine de direction Relations internationales, Législation, Cantons

Team

Chef: Walter Jean-Philippe

Lenman Catherine, juriste

Liste des abréviations

AFAPDP	Association francophone des autorités de protection des données
AFC	Administration fédérale des contributions
AFD	Administration fédérale des douanes
AFF	Administration fédérale des finances
AFS	Archives fédérales suisses
AIEP	Autorité indépendante d'examen des plaintes en matière de radio-télévision
ARE	Office fédéral du développement territorial
ASR	Autorité fédérale de surveillance en matière de révision
AVS	Assurance-vieillesse et survivants
BFC	Bureau fédéral de la consommation
BFEG	Bureau fédéral de l'égalité entre femmes et hommes
BN	Bibliothèque nationale suisse
BPA	Bureau de prévention des accidents
BPH	Brussels Privacy Hub
CAF	Commission arbitrale fédérale
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CER-CN	Commissions de l'économie et des redevances du Conseil national
CFMJ	Commission fédérale des maisons de jeu
ChF	Chancellerie fédérale
CICR	Comité international de la Croix Rouge
CIP-CN	Commissions des institutions politiques du Conseil national
CNPT	Commission nationale de prévention de la torture
COMCO	Commission de la concurrence
ComCom	Commission fédérale de la communication
CSI	Centre de services informatiques
CTI	Commission pour la technologie et l'innovation
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
EAR	Échange automatique de renseignements
EDPP	Échange automatique des déclarations pays par pays
fedpol	Office fédéral de la police
FNS	Fonds national suisse
GPEN	Global Privacy Enforcement Network
ICDPPC	Conférence internationale des commissaires à la protection des données
IFFP	Institut fédéral des hautes études en formation professionnelle
IFSN	Inspection fédérale de la sécurité nucléaire
IPI	Institut Fédéral de la Propriété Intellectuelle
ISDC	Institut suisse de droit comparé
Loi e-ID	Loi fédérale sur les moyens d'identification électronique reconnus par l'État

LRens	Loi fédérale sur le renseignement
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
METAS	Eidgenössisches Institut für Metrologie
MNS	Musée national suisse
MPC	Ministère public de la Confédération
NAVS13	Numéro AVS à 13 chiffres
OBI	Organisation de l'infrastructure ferroviaire
OCDE	Organisation de Coopération et de Développement Économiques
OFAC	Office fédéral de l'aviation civile
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFC	Office fédéral de la culture
OFCL	Office fédéral des constructions et de la logistique
OFCOM	Office fédéral de la communication
OFEN	Office fédéral de l'énergie
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFL	Office fédéral du logement
OFPER	Office fédéral du personnel
OFPP	Office fédéral de la protection de la population
OFROU	Office fédéral des routes
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFSPD	Office fédéral du sport
OFT	Office fédéral des transports
Orens	Ordonnance sur le renseignement
OSAV	Office fédéral de la sécurité alimentaire et des affaires vétérinaires
PostCom	Commission fédérale de la poste
Publica	Caisse fédérale de pensions
RFA	Régie fédérale des alcools
RIPOL	Système de recherches informatisées de la police
SECO	Secrétariat d'Etat à l'économie
SEFRI	Secrétariat d'Etat à la formation, à la recherche et à l'innovation
SEM	Secrétariat d'Etat aux migrations
SFI	Secrétariat d'Etat aux questions financières internationales
SG	Secrétariat général
SIS	Système d'information Schengen
SIS II	Système d'information de Schengen de deuxième génération
SPR	Surveillance des prix
SRC	Service de renseignement de la Confédération
SUVA	Caisse nationale suisse d'assurance en cas d'accidents
UPIC	Unité de pilotage informatique de la Confédération
UTP	Union des transports publics
VIS	Système d'information sur les visas
ZIVI	Organe d'exécution du service civil

Impressum

Ce rapport est également disponible sur Internet (www.leprepose.ch)

Distribution: OFCL, Vente des publications fédérales, CH-3003 Berne
www.bundespublikationen.admin.ch

No d'art. 410.024.f

Mise en page: Duplex Design GmbH

Photographie: Maya Valentin

