



Rapport d'activités 2016/2017

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 2016 au 31 mars 2017.



Table des matières

Avant-propos

Défis actuels et priorités

| | | |
|-----|---|---|
| I | Évolution du contexte technologique et sociétal | 6 |
| II | Extension et accélération de l'activité de contrôle du PFPDT | 7 |
| III | Évolution des attentes du PFPDT | 7 |
| IV | Coopération du PFPDT au niveau national et international | 8 |
| V | Mesures mises en place par le PFPDT pour accroître son efficacité | 8 |

1 Protection des données

1.1 Droits fondamentaux **12**

| | | |
|-------|--|----|
| 1.1.1 | Utilisation du numéro AVS dans les registres: identifiant unique vs sectoriel | 12 |
| 1.1.2 | Destruction et effacement des données récoltées au cours des recensements de la population | 12 |
| 1.1.3 | Établissement des faits auprès de l'Office fédéral du personnel et de l'Office fédéral des constructions et de la logistique | 13 |
| 1.1.4 | Service national d'adresses | 13 |
| 1.1.5 | Enregistrements vidéo dans les piscines à des fins d'entraînement | 14 |

1.2 Protection des données – Questions d'ordre général **15**

| | | |
|-------|--|----|
| 1.2.1 | Révision de la loi fédérale sur la protection des données | 15 |
| 1.2.2 | Stratégie Suisse numérique | 16 |
| 1.2.3 | Transports publics: mise en œuvre de la recommandation concernant le SwissPass et poursuite du conseil | 17 |
| 1.2.4 | Billetterie électronique | 17 |

1.3 Internet et télécommunication **19**

| | | |
|-------|---|----|
| 1.3.1 | Clôture de l'établissement des faits concernant Windows 10 | 19 |
| 1.3.2 | Nouvelles dispositions de Swisscom en matière de protection des données | 19 |
| 1.3.3 | Protocole Internet IPv6 et protection des données | 20 |

1.4 Justice, Police, Sécurité **21**

| | | |
|-------|---|----|
| 1.4.1 | Loi sur l'identification électronique | 21 |
| 1.4.2 | Surveillance de la correspondance par poste et télécommunication – Révision totale des ordonnances du Conseil fédéral | 21 |
| 1.4.3 | Groupe de coordination des autorités suisses de protection des données dans le cadre de Schengen | 22 |

1.5 Santé et recherche **23**

| | | |
|-------|---|----|
| 1.5.1 | Dispositions d'exécution relatives à la loi fédérale sur le dossier électronique du patient | 23 |
| 1.5.2 | Projet BAGSAN de l'Office fédéral de la santé publique | 23 |
| 1.5.3 | Externalisation de la facturation dans le domaine médical | 24 |

1.6 Assurances **25**

| | | |
|-------|---|----|
| 1.6.1 | La libération du secret médical dans le cadre d'une procédure AI | 25 |
| 1.6.2 | Contrôle des services de réception de données des assureurs-maladie | 26 |
| 1.6.3 | Zentrales Informationssystem zur Bekämpfung von Versicherungsmissbrauch | 26 |
| 1.6.4 | Explications relatives aux capteurs fitness en lien avec les assurances | 27 |

| | | |
|-------------|--|-----------|
| 1.7 | Secteur de travail | 28 |
| 1.7.1 | Examen des faits concernant la gestion électronique du recrutement et les dossiers de candidature dans l'administration fédérale | 28 |
| 1.8 | Économie et commerce | 29 |
| 1.8.1 | Privacy Shield entre la Suisse et les États-Unis | 29 |
| 1.8.2 | Agence de renseignements économiques et de crédit Moneyhouse – Action auprès du Tribunal administratif fédéral | 30 |
| 1.8.3 | Ordonnances pour la mise en œuvre du premier train de mesures de la Stratégie énergétique 2050 | 30 |
| 1.9 | Finances | 32 |
| 1.9.1 | Communication de données personnelles à des autorités fiscales étrangères | 32 |
| 1.10 | International | 36 |
| 1.10.1 | Coopération internationale | 36 |
| 1.10.2 | Groupes de coordination de contrôle SIS II, VIS et Eurodac | 38 |
| 1.10.3 | Groupe de travail «Border, Travel & Law Enforcement» | 38 |
| 1.10.4 | Groupe de travail sur la protection des données et l'action humanitaire internationale | 39 |
| 2 | Principe de la transparence | |
| 2.1 | Demandes d'accès | 42 |
| 2.1.1 | Départements et offices fédéraux | 42 |
| 2.1.2 | Services parlementaires | 42 |
| 2.1.3 | Ministère public de la Confédération | 42 |
| 2.2 | Demandes en médiation | 43 |
| 2.3 | Consultations des offices | 44 |
| 2.3.1 | Restriction du principe de la transparence dans le domaine de la surveillance des transports publics | 44 |
| 2.3.2 | Accès aux documents relatifs aux marchés publics | 44 |
| 2.3.3 | Ordonnance sur le Service de renseignement | 45 |
| 2.4 | Varia | 46 |
| 2.4.1 | Nouvelle méthode de travail concernant la tenue des procédures de médiation | 46 |
| 2.4.2 | Les dix ans de la loi sur la transparence | 46 |
| 3 | Le PFPDT | |
| 3.1 | Tâches et ressources | 48 |
| 3.2 | 11^e journée de la protection des données – Les limites de la vidéosurveillance | 50 |
| 3.3 | Publications et participation à des manifestations | 50 |
| 3.4 | Statistiques | 52 |
| 3.4.1 | Statistiques des activités du PFPDT du 1 ^{er} avril 2016 au 31 mars 2016 | 52 |
| 3.4.2 | Statistique des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier 2016 au 31 décembre 2016 | 53 |
| 3.5 | Le Secrétariat du PFPDT | 60 |
| | Liste des abréviations | 62 |



Avant-propos

À l'heure actuelle, pratiquement tous les pays du monde cherchent à saisir les opportunités offertes par la numérisation et à en faire profiter leur population. En particulier dans les domaines des transports et de la santé, la Suisse mène elle aussi de grands projets dans lesquels on attend de nous, en tant que citoyens, dans nos rôles quotidiens de clients, patients ou voyageurs, que nous fournissons une grande quantité de données.

Notre aval à cette évolution et notre confiance dans l'expérience numérique dépendront de la direction prise: celle de pratiques transparentes, équitables et respectueuses des minorités, ou celle de la mise sous tutelle numérique, de la surveillance permanente et des pratiques abusives.

Pour contrer toute dérive néfaste, les autorités et les entreprises mettent en place, en amont des projets, des mesures de protection des données destinées à garantir que la télématique et la robotique viennent appuyer, plutôt que menacer, le droit de tout individu à la liberté et à l'autodétermination. Au vu de la réalité expérimentale de la numérisation, je suis convaincu qu'il faut non seulement mettre en place une nouvelle réglementation, mais également pratiquer une protection des données pragmatique et créative, pour garantir l'acceptation et l'efficacité des nouveaux instruments juridiques et techniques de protection de la sphère privée et de l'autodétermination informationnelle. Par ailleurs, la protection des données doit pouvoir s'appuyer sur des compétences et des moyens crédibles, afin qu'elle puisse valablement accompagner de grands projets et assurer une densité adéquate des contrôles.

Adrian Lobsiger

Préposé fédéral à la protection des données et à la transparence

Défis actuels et priorités

I Évolution du contexte technologique et sociétal

Le 21 décembre 2016, le Conseil fédéral a mis en consultation l'avant-projet de révision totale de la loi fédérale sur la protection des données (AP-LPD). L'objectif visé par le Conseil fédéral est de «renforcer la protection des données et [de] l'adapter aux technologies et à la société d'aujourd'hui». Ces évolutions sont décrites brièvement ci-après.

Technologie et économie

Depuis l'arrivée sur le marché du premier iPhone en 2007, la dynamique du développement des technologies de l'information et de la communication (TIC) n'a cessé de s'accroître. Après les smartphones, de plus en plus d'appareils du quotidien sont équipés de processeurs, capteurs et modules réseau performants. Ces appareils échangent sur Internet de grandes quantités de données sur leurs utilisateurs et leur environnement, parfois même sans interactions avec les utilisateurs. Le traitement de ces données est opéré dans des centres de calcul répartis dans le monde entier, selon des procédures (algorithmes) aux finalités les plus diverses. Les progrès de la technologie sont tels que les performances de certains systèmes sont qualifiées d'«intelligence artificielle», car ils sont capables de réagir de façon autonome sans impulsions directes des individus et en temps réel.

Les acquis technologiques des TIC ne seraient pas si omniprésents sans l'économie mondialisée, qui a développé un modèle économique reposant sur la collecte, l'analyse et la transmission d'importants volumes de données (Big Data), et qui propose aux ménages et aux entreprises des dispositifs TIC de plus en plus performants et de moins en moins coûteux.

Société, politique et droit

La pénétration du monde des loisirs et du travail par des TIC toujours plus compactes, ainsi que les modes de vie toujours plus connectés dus à l'omniprésence des smartphones ont fait de la numérisation un phénomène de société. Entre autres effets bénéfiques ou néfastes, le rapport de la société aux TIC induit des risques d'incursions indésirables dans l'autodétermination informationnelle et dans la sphère privée des individus, pouvant aller jusqu'à la perte de contrôle sur d'importants volumes de données.

La numérisation a été accélérée par la libéralisation des marchés mondiaux de la télécommunication et la chute des prix des composants électroniques, entraînant une multiplication des prestataires actifs à l'échelle

internationale. Les entreprises de TIC comptent aujourd'hui parmi les sociétés les plus dotées en capital, et leurs marchés sont les plus lucratifs au monde. Elles gagnent des clients partout sur la planète grâce à des offres «gratuites» et génèrent ainsi d'énormes fichiers de données, dont elles tirent des profits considérables grâce au modèle économique du «Big Data» – modèle qui fait des émules et s'impose progressivement dans tous les pans de l'économie. Par l'exploitation d'immenses fichiers de données, à la croissance toujours plus rapide, les entités qui traitent ces données génèrent des connaissances permettant à présent de reconstituer les modes de comportements et les préférences des milliards d'individus utilisant chaque jour leurs services en ligne. En réponse à cette évolution, le Conseil de l'Europe avec la Convention 108 et l'UE avec le Règlement général sur la protection des données (RGPD) ont posé les jalons pour un droit unifié sur la protection des données, qui déploie également ses effets sur des États tiers comme la Suisse et les États-Unis grâce à ses instruments pour la préservation d'un niveau équivalent de protection. Pour l'essentiel, ces instruments visent les objectifs suivants:

- obliger les prestataires d'offres en ligne captant de gros volumes de données à publier la nature, le contenu et l'étendue des données collectées. Les clients doivent savoir quels traitements vont au-delà de l'utilisation fiable d'une application de base et le cas échéant, avoir la possibilité de les exclure ou d'y mettre un terme en cas de refus;
- renforcer les compétences des responsables de la protection des données et les obliger à réduire en amont de tout projet le risque d'atteintes à la personnalité, conformément aux principes de la protection de la vie privée dès la conception («privacy by design», intégration de la protection des données dès la phase de projet) et de la protection de la vie privée par défaut («privacy by default», paramétrage par défaut conforme à la protection des données);
- promouvoir l'interaction entre les services internes de protection des données des entreprises et des administrations avec les autorités en charge de la protection des données;
- étendre les prérogatives des autorités de protection des données et adapter leurs méthodes de travail à l'interaction accrue avec les responsables d'applications.

Comme nous allons l'exposer à présent, le contexte technologique et sociétal décrit ci-dessus pose une série de défis auxquels est confrontée l'autorité de protection des données de la Confédération:

II Extension et accélération de l'activité de contrôle du PFPDT

Le concept du Big Data se développe non seulement dans l'économie privée, soumise à la surveillance du PFPDT, mais également dans l'administration fédérale et les entreprises publiques, qui gèrent ou développent une grande diversité d'applications reposant sur d'importants fichiers de données, alimentés par les citoyens dans leurs rôles quotidiens de clients, patients ou voyageurs. Même si les responsables des fichiers de données ainsi constitués n'exploitent que rarement ou partiellement le caractère personnel de ces données, les performances des moteurs de recherche modernes créent un risque d'identification rétroactive des individus. Le PFPDT doit donc étendre son activité de surveillance à de nombreux projets des autorités fédérales et de l'économie qui poursuivent des objectifs scientifiques, statistiques, techniques ou administratifs sans relier les données à des personnes. Il doit s'assurer que les informations collectées soient anonymisées d'une façon qui exclut, avec une probabilité suffisante, toute identification rétroactive au moyen des technologies actuelles. Comme les données anonymisées peuvent également être recoupées avec des informations accessibles sur Internet, ce travail s'avère extrêmement difficile et chronophage pour le PFPDT. Les projets en question doivent faire l'objet d'un accompagnement interdisciplinaire, c'est-à-dire juridique et technique.

Les applications destinées à traiter les données personnelles ne sont aujourd'hui plus livrées pour être installées localement, mais accessibles sur Internet, et constamment mises à jour par de nouvelles fonctions, p. ex. de protection en ligne contre les logiciels malveillants. Cela signifie que les contrôles se complexifient à mesure que les applications évoluent, et doivent être opérés à un rythme toujours plus soutenu.

III Évolution des attentes du PFPDT

Le style de vie de la société numérique se caractérise par une insouciance dans le rapport aux TIC, qui peut se changer brutalement en tempête d'indignation dès que les médias ou les organisations de défense des consommateurs dénoncent des risques d'incursions dans la vie privée liés à une application grand public. Le grand public attend du PFPDT, a minima, qu'il l'informe concernant les risques que comportent les applications les plus courantes, souvent disponibles gratuitement sur Internet. Dans le même temps, le PFPDT est censé communiquer

sur les possibilités de protection de la vie privée et garantir la conformité des applications grand public avec les normes de protection des données dans le cadre de procédures de surveillance.

Au vu du grand nombre d'utilisateurs, ces attentes de la population suisse sont justifiées. Le PFPDT a donc intégré dans son activité d'information et de surveillance la culture en ligne et les applications destinées aux consommateurs. La crédibilité du PFPDT en tant qu'autorité spécialisée suppose donc une analyse du fonctionnement des technologies plus approfondie, allant au-delà des faits présentés dans les médias. Pour répondre aux besoins les plus pressants, le PFPDT a ouvert une hotline, renforcé ses ressources humaines en informatique et mis en place un laboratoire informatique rudimentaire, lui permettant de tester la conformité en termes de protection des données des applications pour smartphone les plus courantes et d'autres offres en ligne.

À la demande d'entreprises privées et de régies fédérales, le PFPDT a commencé à pratiquer un accompagnement consultatif de grands projets impliquant le traitement d'importants volumes de données personnelles. Ce besoin d'un accompagnement des projets le plus en amont possible découle de l'évolution du mode de travail des services juridiques et de protection des données, qui contrôlent la conformité des projets dès leurs premières étapes, comme le prescrit le principe de *privacy by design* instauré dans l'AP-LPD.

Le contrôle par le PFPDT d'applications déjà existantes peut entraîner pour les entreprises qui les conçoivent des corrections coûteuses et néfastes pour leur réputation, si bien que le principe du *privacy by design* est bien accueilli par bon nombre d'entre elles, en particulier si cette méthode peut être corrélée avec une évaluation phase par phase des principales étapes du projet par l'autorité de protection des données. Pour le PFPDT, ce mode de travail associant rôle consultatif et surveillance présente l'avantage de pouvoir réduire en amont les risques en matière de protection des données. Ainsi, l'autorité peut également intervenir sur des applications en ligne à courte durée de vie, ce qui s'avère beaucoup plus simple que dans le cadre de longue procédure de décisions ou de sanctions.

Les exemples actuels d'interventions de ce type sont les grands projets *Mobility Pricing*, des régies de transports publics et du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), *Sesam* de la Poste et des CFF, *TWINT* de la Poste et d'établissements bancaires, ou *Admeira* de Swisscom, la SSR et Ringier.

IV Coopération du PFPDT au niveau national et international

Comme les autorités de protection des données de la Confédération et des cantons sont bien souvent confrontées aux mêmes évolutions et aux mêmes technologies de traitement des données personnelles, le PFPDT entend intensifier ses interactions avec les préposés cantonaux à la protection des données. La collaboration intercantonale est coordonnée par l'association «privatim».

Un exemple révélateur de la nécessité d'une étroite collaboration est l'introduction prévue par le Conseil fédéral du numéro AVS non parlant à 13 chiffres comme identificateur universel dans les administrations fédérales, cantonales et communales. Il paraît évident que les risques technologiques d'identification rétroactive indésirable qu'implique ce projet doivent faire l'objet d'une évaluation commune par la Confédération et les cantons.

À l'échelle internationale, les prochaines tâches du PFPDT seront les suivantes:

Privacy Shield

Avec le développement d'Internet et la prédominance de l'industrie informatique californienne, qui gère de gigantesques centres de calcul ou des clouds, traitant les données biométriques et d'autres données personnelles de millions d'utilisateurs suisses, l'évaluation des transferts de données personnelles vers l'étranger a pris une place considérable dans l'activité de surveillance du PFPDT. Pour que le nouveau cadre juridique «Privacy Shield» conclu en janvier 2017 entre la Suisse et les États-Unis, contrairement au précédent accord «Safe Harbor» invalidé par la CJUE, puisse se pérenniser et s'adapter à l'évolution des besoins, des évaluations annuelles ont été convenues avec les États-Unis. Ces évaluations seront menées par le SECO, assisté du PFPDT, qui produira un rapport annuel indépendant.

Communautarisation de la protection des données dans l'UE

Le 1^{er} mai 2018, l'UE mettra en vigueur son Règlement général sur la protection des données (RGPD), que les responsables d'applications en Suisse devront également respecter dans la mesure où ils traitent des données de citoyens de l'UE. Ce règlement remplacera les législations en matière de protection des données des différents États membres de l'UE. Les autorités nationales de protection des données devront à l'avenir coordonner plus étroitement leurs activités de surveillance.

Au vu de la communautarisation de la protection des données et de l'application extra-territoriale du RGPD, on peut s'attendre à ce que l'UE souhaite exercer un droit de regard sur la façon dont les États tiers

mettent en application les principes qu'il contient. La Suisse sera tout particulièrement l'objet de cette attention, car, en tant que membre associé du dispositif Schengen-Dublin, elle échange de grandes quantités de données administratives sensibles avec l'UE.

Dans ce contexte, il est clair que le PFPDT doit se profiler comme premier interlocuteur pour les organes indépendants de protection des données de l'UE et de ses États membres. Pour cela, il doit être représenté de façon adéquate lors des divers événements internationaux sur ce thème et être en mesure de couvrir les dépenses y relatives. Et ce, également, au regard de la Directive UE 2016/680, qui exige que le PFPDT soit associé aux travaux du comité européen de la protection des données.

V Mesures mises en place par le PFPDT pour accroître son efficacité

Pour être en mesure de relever les défis qui s'imposent à lui et de répondre aux attentes correspondantes de l'économie et de l'administration, ainsi que du grand public, le PFPDT a introduit au cours de l'exercice 2016/2017 une série de mesures visant une utilisation plus efficace des moyens dont il dispose.

- Au vu des défis décrits plus haut, le PFPDT a défini les priorités stratégiques suivantes:
- renforcement de ses propres compétences concernant les technologies ainsi que les modèles économiques et de communication de la société numérique;
- accompagnement consultatif de projets pertinents des autorités et de l'économie;
- présence visible pour les citoyens suisses concernés.

Sur la base de cette stratégie, un plan a été élaboré pour l'année 2017, prévoyant l'accompagnement consultatif de dix grands projets ainsi que huit opérations de contrôle de grande envergure (cf. chiffre 3.1 du présent rapport).

Réorganisation de l'autorité de protection des données

L'accent stratégique et opérationnel mis sur la numérisation est appuyé par une réorganisation de l'autorité, qui a pris effet le 1^{er} avril 2017 et est neutre en termes de coûts. Elle vise à renforcer les compétences techniques du PFPDT et à décharger sa direction d'un certain nombre de tâches transversales courantes:

Toutes les tâches de direction traditionnelles et transversales, telles que le contrôle des affaires, la communication et les finances, ont été transférées dans une nouvelle unité appelée Centres de compétences

(cf. l'organigramme du PFPDT: www.leprepose.ch, Le PFPDT – Organisation).

Les deux anciennes unités chargées de l'application de la LPD ont été regroupées en trois équipes chapeautées par une même direction.

Un laboratoire nouvellement mis en place permet de tester des applications consommateurs, des produits TIC ou des réseaux sociaux.

Remaniement conceptuel de l'offre d'information

En 2016, le PFPDT a répondu à environ 3500 demandes orales ou écrites de citoyens, d'entreprises et d'organisations. De plus, il a publié sur son site une offre étendue d'informations sur les évolutions technologiques, avec des conseils pratiques, ainsi que l'ensemble des recommandations formelles formulées dans le cadre de son activité de surveillance. Cette offre a été soumise, tout comme le rapport d'activités, à un remaniement conceptuel. Le PFPDT entend ainsi répondre au mieux au besoin croissant, exprimé par le grand public, d'information proactive sur les applications techniques courantes.

Adaptation de la procédure dans le domaine de la loi sur la transparence (LTrans)

Ces dernières années, l'unité LTrans a accumulé des retards importants dans le traitement des demandes en médiation. Pour éviter d'avoir à transférer du personnel depuis l'unité LPD pour venir à bout de ces retards, comme cela a été nécessaire par le passé, le PFPDT a mis en place à compter du 1^{er} janvier 2017 une procédure sommaire et accélérée, caractérisée par des procédures de médiation orales (cf. chiffre 3.1 du présent rapport).



Protection des données

1.1 Droits fondamentaux

1.1.1 Utilisation du numéro AVS dans les registres: identifiant unique vs sectoriel

Au cours de l'année sous revue, nous avons conseillé les commissions des affaires juridiques du Conseil national et du Conseil des États concernant l'introduction du numéro AVS dans le registre du commerce et dans le registre foncier. Nous nous sommes par ailleurs prononcés sur le projet de permettre systématiquement l'utilisation du numéro AVS en-dehors du domaine des assurances sociales.

Nous préconisons depuis des années l'utilisation d'identifiants sectoriels (cf. notamment notre 22^e rapport d'activités 2014/2015, chiffres 1.1.2 et 1.1.3). Le Conseil fédéral et le Parlement ont également retenu cette solution pour le numéro d'identification du patient selon la loi fédérale sur le dossier électronique du patient. De même, avec la promulgation des dispositions révisées sur le registre du commerce dans le droit des obligations, le législateur a créé le 17 mars 2017 un identifiant sectoriel qui sera également visible à l'extérieur lors de la circulation des registres. Cette solution permet l'identification univoque des personnes inscrites dans le registre, tout en apportant une réponse à nos préoccupations quant à la possibilité de mise en relation abusive de données personnelles. L'Office fédéral du registre du commerce sera chargé de générer ces numéros.

Au cours de l'année sous revue, nous avons été consultés dans les commissions des affaires juridiques du Conseil national et du Conseil des États, non seulement sur le projet de loi sur le registre du commerce, mais également sur la révision du registre foncier. Le Conseil des États s'est prononcé pour l'utilisation d'un numéro sectoriel pour le registre foncier, par analogie au registre du commerce, et cette question sera traitée au début de l'été 2017 par la commission des affaires juridiques du Conseil national.

Après que des identifiants sectoriels ont été introduits dans les domaines de la santé et des registres, le Conseil fédéral a demandé le 1^{er} février 2017 au Département fédéral de l'intérieur d'élaborer un projet de loi destiné à faciliter l'utilisation systématique des numéros AVS par les autorités fédérales, cantonales et communales au-delà du domaine des assurances sociales. Nous voyons dans ce projet un changement de direction, ou tout du moins une incohérence par rapport aux solutions sectorielles décrites précédemment.

Nous n'avons cessé de souligner le risque de dommage auquel l'utilisation généralisée du numéro AVS en dehors du domaine des assurances sociales exposerait

intégralement et simultanément les administrations fédérales, cantonales et communales en cas de fuites ou de manipulations illicites de données. Par ailleurs, nous avons exprimé des doutes quant à la pertinence d'utiliser précisément le numéro AVS comme identifiant multisectoriel et quant à la sûreté de cette solution, alors même que ce numéro circule dans toutes les entreprises privées.

En réponse à ces observations, l'administration objecte que, au vu des performances des moteurs de recherche modernes, les risques en matière de protection des données ne sont pas plus élevés avec une utilisation généralisée du numéro AVS qu'avec l'utilisation d'identifiants sectoriels. Comme nous l'avons exposé lors de nos auditions devant les commissions parlementaires, nous ne sommes pas fermés à cette argumentation. Il revient cependant à l'administration – en tant qu'initiatrice des risques – de prouver par des faits scientifiquement établis qu'une réévaluation de ces risques est effectivement indiquée du fait des progrès techniques.

Comme le changement de système visé concerne toutes les collectivités de Suisse et les données personnelles de millions de personnes, nous exigeons qu'une instance spécialisée indépendante réalise une analyse d'impact. Les organes de protection des données de la Confédération et des cantons devront ensuite pouvoir prendre position sur cette étude.

1.1.2 Destruction et effacement des données récoltées au cours des recensements de la population

Au cours de l'exercice écoulé, en mars 2016, nous avons engagé une procédure d'établissement des faits auprès de l'Office fédéral de la statistique (OFS). Cet examen porte essentiellement sur le contrôle de la destruction et de l'effacement des données collectées pour le recensement de la population.

Nous voulions savoir comment l'OFS efface ou détruit les données de recensement, après leur saisie, leur correction et leur contrôle. Nous estimions nécessaire de considérer de plus près les processus utilisés dans ce contexte et de les examiner sous l'angle de leur conformité avec la loi sur la protection des données (LPD). Nous avons déjà effectué une visite sur place à l'OFS. Notre prochaine étape sera l'analyse des documents reçus de l'OFS ainsi que les réponses à nos questions; nous vérifierons par ailleurs si les processus cités répondent aux exigences de la LPD.

1.1.3 Établissement des faits auprès de l'Office fédéral du personnel et de l'Office fédéral des constructions et de la logistique

Nous avons mené deux contrôles auprès de l'Office fédéral du personnel (OFPER) et de l'Office fédéral des constructions et de la logistique (OFCL) concernant une partie de l'utilisation de l'infrastructure électronique de la Confédération et nous sommes arrivés à la conclusion que les durées de conservation des données appliquées respectent les exigences légales.

Durant l'année sous revue, nous avons, dans le cadre de nos activités de surveillance, procédé à des vérifications concernant le respect de la durée de conservation et le processus de destruction des données administrées conformément à l'article 4 de l'ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération.

Le but de ce contrôle était de comprendre comment la destruction de ces données intervient concrètement et d'évaluer si les délais de conservation étaient en l'espèce respectés. Dans ce contexte, nous avons décidé l'ouverture de deux procédures d'éclaircissement. La première auprès de l'OFPER pour ce qui concerne les données concernant le temps de travail du personnel au sens de la loi sur l'organisation du gouvernement et de l'administration (LOGA) et dont la durée de conservation est de cinq ans au plus. La seconde procédure a été ouverte auprès de l'OFCL pour les données concernant la présence des personnes dans les locaux de la Confédération ainsi que les entrées et les sorties et dont la durée de conservation est de trois ans au plus.

Notre analyse de la situation n'ayant pas permis de conclure à d'éventuels manquements concernant la durée de conservation prévue dans l'ordonnance précitée, nous avons clos nos contrôles sans émettre de recommandations. En effet, il a pu être constaté que, même si elles ne sont pas réglées de façon uniforme au sein de l'administration fédérale, les durées de conservation ne sont pas supérieures aux délais fixés par l'ordonnance et respectent par conséquent les exigences figurant dans la loi sur la protection des données.

1.1.4 Service national d'adresses

Nous avons pris connaissance de l'étude mandatée par le Conseil fédéral concernant la création d'un registre national d'adresses. Nos remarques émises dans le cadre de la consultation des offices y relative ont été pour l'essentiel prises en compte. Nous continuons à suivre le projet avec attention.

Le 12 novembre 2014, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'examiner les différentes possibilités de créer un registre national d'adresses et de lui soumettre une proposition avant fin 2016 (cf. notre 23^e rapport d'activités 2015/2016, chiffre 1.1.3).

L'étude, conduite par un expert mandaté par l'Office fédéral de la justice (DFJP), est parvenue à la conclusion que la solution optimale consistait à créer un registre au niveau fédéral (le service national d'adresses – SNA) utilisant les données d'adresses actuellement récoltées par l'Office fédéral de la statistique (OFS) à des fins statistiques. Il s'agira alors de créer une passerelle assurant le transfert de données de l'OFS vers le SNA. L'organisation du SNA sera indépendante du registre actuellement géré par l'OFS. Les coûts pourront être couverts par la perception d'un émolument. Du point de vue juridique, la création du SNA pourra s'effectuer suite à la modification de la loi sur l'harmonisation des registres (LHR). Les détails techniques et organisationnels du SNA doivent encore être précisés.

Le Conseil fédéral doit se prononcer sur la création du SNA et mandater le DFJP afin qu'il lui soumette avec le soutien technique de l'OFS d'ici à fin 2018 un projet destiné à la consultation externe.

Dans le cadre de la consultation des offices, nous avons été invités à prendre position sur le rapport de suivi concernant l'échange de données d'adresses entre les registres des habitants et d'autres détenteurs de données. Nos remarques ont pour l'essentiel été prises en considération. Celles-ci portaient sur les finalités exactes d'un tel service, le rôle de l'OFS – garant du secret statistique et d'une utilisation des données conforme à son mandat légal, la durée de conservation des adresses, le cercle des utilisateurs autorisés, la proportionnalité de la collecte des données, l'exactitude des données en cas d'actualisation non immédiate, sur l'organisation du SNA et de l'autorité de surveillance ainsi que sur les mesures techniques et organisationnelles prises afin de garantir la protection des données.

En tant que membres du groupe de travail, nous continuons de suivre avec attention ce projet et nous assurerons qu'au vu des précisions techniques et organisationnelles qui seront encore apportées par la suite que la variante proposée respecte la protection des données.

1.1.5 Enregistrements vidéo dans les piscines à des fins d'entraînement

La réalisation d'enregistrements vidéo dans une piscine peut empiéter sur la sphère intime des baigneurs. Il convient, lors de séances d'entraînement nécessitant de telles prises de vue, de s'assurer qu'aucun baigneur non concerné ne se trouve dans la zone filmée.

L'analyse de vidéos s'est imposée comme outil d'entraînement dans diverses disciplines sportives. Elle est utile par exemple pour optimiser les séquences de mouvements des sportifs. Il n'est donc pas étonnant que les entraîneurs de natation y fassent également recours. Lorsqu'un entraînement de natation a lieu dans une piscine publique, cela peut toutefois générer une situation problématique au regard de la protection de la personnalité.

Les prises de vue effectuées sous l'eau dans une piscine publique peuvent constituer une intrusion dans la sphère intime des personnes concernées, que les seuls objectifs sportifs ne peuvent pas justifier. C'est pourquoi elles requièrent le consentement explicite de toutes les personnes concernées. Obtenir le consentement des sportifs filmés ne pose a priori pas de problème. Une fiche d'information a été publiée sur ce thème par l'Office fédéral du sport (OFSP): www.mobilesport.ch

En revanche, pour les baigneurs qui ne participent pas à l'entraînement, le consentement explicite peut être plus difficile à recueillir. Pour être valable, un consentement suppose que les personnes concernées aient été informées de tous les aspects de l'enregistrement vidéo. Elles doivent être informées que des prises de vue seront effectuées, mais aussi de leur but, de leur durée de conservation et des personnes qui vont visionner ces vidéos. De plus, le consentement doit être donné librement, c'est-à-dire que les personnes concernées doivent aussi pouvoir utiliser la piscine sans être filmées.

En pratique, ces conditions sont quasiment impossibles à remplir dans une situation de fonctionnement normal de la piscine: il n'est pas envisageable d'informer suffisamment tous les baigneurs susceptibles de se retrouver par hasard dans la zone filmée et de respecter leur éventuel refus d'être filmés. C'est pourquoi les personnes chargées du traitement des données doivent s'assurer que seuls les participants à l'entraînement se trouvent dans les secteurs concernés. Pour cela, on peut par exemple envisager d'utiliser la vidéo à des fins d'analyse uniquement en-dehors des horaires d'ouverture officiels de la piscine.

1.2 Protection des données – Questions d’ordre général

1.2.1 Révision de la loi fédérale sur la protection des données

Le 21 décembre 2016, le Conseil fédéral a mis en consultation l’avant-projet de révision de la loi fédérale sur la protection des données. L’objectif de cette révision est d’adapter notre législation aux nouvelles technologies, de renforcer la protection des données et l’attractivité de la Suisse pour le numérique. La loi révisée doit en particulier se rapprocher des nouveaux standards européens et maintenir la reconnaissance d’un niveau de protection des données adéquat. Pour nous, il est important que cette révision aboutisse rapidement.

La loi fédérale sur la protection de données (LPD) fait partie des législations de protection des données de la première génération. Elle précède l’arrivée d’Internet, des téléphones intelligents et de l’internet des objets. Même si ce texte n’est en aucun cas dépassé, une révision s’impose pour répondre aux nouveaux défis de la société numérique et mieux garantir le respect des droits et des libertés fondamentales des personnes lors du traitement de données personnelles les concernant. Une révision est également fondamentale pour répondre à la réforme du cadre juridique européen et notamment la modernisation de la Convention du Conseil de l’Europe pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel (Convention 108). Sur mandat du Conseil fédéral, l’Office fédéral de la justice a préparé un projet de révision totale de la LPD. Ce projet a été mis en consultation par le Conseil fédéral le 21 décembre 2016.

Nous avons participé aux travaux de révision et fait valoir notre point de vue au sein du groupe de travail et lors de la procédure de consultation des offices. Le projet répond largement à nos attentes. Toutefois certains points devront être revus pour que notre législation soit parfaitement conforme à la Convention 108 révisée et pour permettre un plus grand rapprochement avec le cadre juridique européen. Un tel rapprochement permettrait d’offrir une plus grande sécurité juridique. Ce serait non seulement à l’avantage des personnes concernées, mais aussi des responsables de traitement et de la place économique suisse.

La révision doit renforcer le droit à la protection des données afin que tout un chacun puisse disposer d’une plus grande maîtrise sur les informations qui le concernent. Cela passe par une plus grande transpa-

rence des traitements et l’octroi de nouveaux droits tel que le droit de pouvoir faire valoir son point de vue avant d’être soumis à une décision automatisée ou le droit de connaître la manière dont de telles décisions sont prises. La révision vise à renforcer et concrétiser les obligations des responsables de traitement. Elle prévoit d’introduire notamment une obligation d’annonce des violations de la protection des données, l’obligation de procéder à des études d’impact de protection des données et une obligation de documenter les traitements. Elle introduit les principes de la protection des données dès la conception (privacy by design) et de la protection des données par défaut (privacy by default).

La révision doit renforcer les compétences du PFPDT qui se verra conférer un pouvoir de décision. Le préposé devrait à l’avenir pouvoir émettre des recommandations de bonnes pratiques (Best practices) élaborées en coopération avec les milieux intéressés; il pourra également approuver ou reconnaître des règles contraignantes d’entreprises (Binding corporate rules, BCR) dans le cadre des transferts de données à l’étranger. De même, il pourra édicter, reconnaître ou approuver des clauses contractuelles standards. Par contre, il incombera au Conseil fédéral de prendre à l’avenir des décisions concernant le niveau de protection adéquat d’un État tiers.

Les possibilités de coopération avec d’autres autorités de protection des données en Suisse et à l’étranger et d’entraide administrative sont également améliorées. Pour que le PFPDT puisse assumer de manière crédible et effective ses tâches actuelles et futures, il devra cependant disposer de ressources et de moyens supplémentaires conséquents, comme le souligne le rapport explicatif concernant l’avant-projet. Il devrait également disposer d’un budget propre similaire au modèle adopté pour le contrôle fédéral des finances ou la nouvelle autorité de surveillance sur le service de renseignement de la Confédération. La révision permet aussi un renforcement significatif des sanctions pénales, même si le projet reste en retrait par rapport aux montants des sanctions prévus dans le règlement européen. Enfin, l’obligation d’annoncer les fichiers ou les traitements dans le secteur privé sera supprimé. Le registre des fichiers ne recensera à l’avenir que les traitements des organes fédéraux.

Tout en saluant la qualité du projet de révision, nous estimons qu’il devrait néanmoins être complété. Ainsi, nous avons proposé lors de la procédure de

consultation des offices, entre autres, de renforcer encore la position des personnes concernées, notamment avec un droit de portabilité des données et un droit au déréférencement complétant le droit à l'effacement. Les responsables de traitements qui présentent un risque particulier d'atteinte à la vie privée devraient être tenus de nommer un conseiller à la protection des données. Cette fonction est déjà largement implémentée dans de nombreuses entreprises, fait l'objet de formations ad hoc et constitue un instrument effectif de la mise en œuvre de la protection dans l'entreprise ou l'administration.

Enfin, la LPD devrait pouvoir aussi s'appliquer à des responsables de traitement qui n'ont pas de siège en Suisse mais qui procèdent à des traitements y déployant des effets et qui concernent des personnes y résidant. Ces responsables de traitement devraient avoir un répondant en Suisse, notamment pour faciliter l'exercice des droits des personnes concernées. La relation entre notre législation et le règlement européen, notamment ses effets en Suisse ou pour des responsables de traitement suisses ayant des activités de traitement en Europe suscitent de nombreuses interrogations légitimes en Suisse et en Europe. En ce sens, nous saluons la motion 16.3752 du Groupe radical libéral «Contre les doublons en matière de protection des données» qui demande au Conseil fédéral d'approcher l'Union européenne en vue d'un accord de coopération concernant l'application des législations respectives.

Nous allons suivre activement l'évolution du projet de révision également suite à la procédure de consultation externe.

1.2.2 Stratégie Suisse numérique

Dans le cadre de consultations des offices et de groupes de travail, nous avons pris position sur la mise en œuvre de la Stratégie Suisse numérique du Conseil fédéral et exposé les exigences en matière de protection des données. Nous entendons veiller à la prévention de tout risque d'atteinte à la personnalité. À cette fin, des mesures de protection doivent être intégrées dès la phase de planification d'un projet.

Avec la Stratégie Suisse numérique, le Conseil fédéral a adopté en 2014 une nouvelle politique en matière de données. Elle vise à exploiter pleinement les atouts de la numérisation afin notamment de positionner la Suisse comme un pôle économique et scientifique innovant et tourné vers l'avenir. Les différentes mesures de la Stratégie sont définies dans un plan d'action.

L'une des mesures de la Stratégie consiste à définir des conditions cadre pour l'économie numérique, qui sont décrites dans un rapport. Lors de la consultation

des offices concernant ce rapport, nous avons indiqué que les aspects juridiques relatifs à la protection des données devaient être examinés dès la phase de planification et de développement des projets d'économie numérique. Dès le début d'un projet, des mesures de protection adéquates doivent être intégrées pour prévenir d'éventuelles violations des prescriptions légales. Cependant, une protection efficace des données présuppose que l'entité chargée de leur traitement sache quelles données il traite et comment. C'est pourquoi nous avons recommandé d'obliger les porteurs de projet à produire une documentation adéquate sur les traitements de données planifiés ainsi qu'une analyse de leurs répercussions potentielles sur les droits des personnes concernées.

Une autre mesure de la Stratégie a été la mise en place d'un groupe de travail chargé de rédiger une note de discussion concernant la politique des données en Suisse. Nous sommes représentés dans ce groupe de travail et avons en particulier souligné la nécessité de garantir la protection des données et de la personnalité à long terme également. Nous avons aussi recommandé d'aménager pour les personnes concernées un droit de décision concernant l'utilisation de leurs données. De plus, nous avons insisté sur l'importance d'une distinction entre données personnelles et données techniques, qui est déterminante pour l'application des dispositions de protection de la LPD.

Par ailleurs, nous avons également pris position concernant le rapport sur la politique économique extérieure 2016 et les messages concernant des accords économiques, ainsi que le rapport concernant les mesures tarifaires prises en 2016. Le rapport examine les opportunités et les défis induits par la mondialisation et la numérisation, sans toutefois aborder dans ce contexte l'aspect essentiel de la protection de la personnalité des personnes concernées. Nous avons signalé que la prise en considération de cet aspect était précisément nécessaire en raison des négociations actuelles sur les accords de libre-échange.

1.2.3 Transports publics: mise en œuvre de la recommandation concernant le SwissPass et poursuite du conseil

Au cours de l'année sous revue, nous avons vérifié la mise en œuvre de notre recommandation et de nos propositions d'amélioration dans le dossier SwissPass. Notre procédure d'établissement des faits est ainsi achevée. Nous continuerons à conseiller le secteur des transports.

Au cours de cette année, nous avons vérifié la mise en œuvre de notre recommandation et de nos propositions d'amélioration en relation avec le SwissPass (cf. chiffre 1.2.1 de notre 23^e rapport d'activités 2015/2016). Il s'agissait principalement de veiller à ce que les données de contrôle relatives au SwissPass d'une part soient effacées, et d'autre part ne soient plus collectées. Sur ce point, nous avons effectué deux contrôles sur place, en présence de représentants des CFF et de l'Union des transports publics (UTP). La mise en œuvre de notre recommandation a notamment impliqué une adaptation du logiciel de l'appareil de lecture des SwissPass. Les différentes entreprises de transport impliquées ont dû l'intégrer et le télécharger. Dans le même temps, les responsables ont effacé rétroactivement les données de contrôle collectées sur les SwissPass. Par ailleurs, toutes les entreprises de transport ont intégré les conditions générales de l'abonnement demi-tarif et de l'abonnement général dans leur version du 1^{er} juin 2016, adaptée conformément à notre proposition d'amélioration.

Notre recommandation du 4 janvier 2016 étant ainsi mise en œuvre, nous avons clôturé notre procédure d'établissement des faits.

Nous restons en contact avec l'UTP et l'ensemble du secteur des transports, pour un accompagnement consultatif. Nous veillerons notamment dans ce cadre à ce que l'évolution future du SwissPass demeure conforme aux impératifs de protection des données. Nous sommes également en contact avec l'Office fédéral des transports (OFT), qui étudie la possibilité d'instaurer une base légale.

1.2.4 Billetterie électronique

La billetterie électronique soulève de nombreuses questions en relation avec la protection des données. La collecte et le traitement des données doivent notamment s'opérer sur une base volontaire et dans le respect du droit à l'information des voyageurs. Cependant, les autres conditions relatives au droit de la protection des données doivent également être prises en compte.

Plusieurs entreprises de transport nous ont consultés dans le contexte de l'introduction de services de billetterie électronique. La billetterie électronique peut prendre différentes formes. Pour pouvoir utiliser les offres, les voyageurs doivent au préalable télécharger une application sur leur appareil mobile et s'inscrire. La saisie des voyages se fait automatiquement, et dans certains cas, les lieux et dates de départ et de destination du voyage doivent être confirmés en appuyant sur une touche. On établit des profils de déplacement des voyageurs, qui sont utilisés pour la facturation.

Chaque système de billetterie électronique doit être contrôlé au regard de sa conformité avec le droit de la protection des données. Nous n'évoquons ci-après que les points les plus importants. Il importe que la collecte des informations se fasse sur une base volontaire, que le voyageur soit informé des traitements qui seront effectués sur les données, et qu'il les autorise. Une révocation de l'autorisation doit être possible en tout temps. Le détenteur des données doit être clairement identifié, mais cette information peut être contenue dans les conditions générales. La personne concernée doit savoir en particulier qui traite quelles données la concernant, et combien de temps ces données sont conservées. Seules les données pertinentes et nécessaires doivent être traitées (principe de proportionnalité).

En principe, les entreprises de transport ne sont pas autorisées à communiquer à des tiers les données de déplacement. Ainsi, par exemple, elles doivent transmettre à une société de carte de crédit chargée de la facturation uniquement le montant global, et non les informations sur les voyages ou les déplacements. Si les données ne sont pas collectées uniquement pour le calcul du prix du billet et la facturation, mais également pour d'autres utilisations, par exemple à des fins de marketing ou d'établissement de profils d'utilisateur, l'information adéquate et l'autorisation de la personne concernée sont là encore requises. Il importe de signaler spécifiquement tout traitement inhabituel des données. Le traitement de profils de déplacement doit en outre être expressément autorisé par l'utilisateur (p.ex. clause d'opting-in par opposition à une clause d'opting-out). Les données personnelles collectées doivent être transmises sous forme cryptée.

Les entreprises de transport doivent également mettre en place des mesures techniques et organisationnelles pour la protection des données. Les données de déplacement doivent être autant que possible pseudonymisées ou anonymisées. Pour la régulation du nombre de passagers et du taux d'utilisation du matériel roulant, des données anonymisées suffisent. Dès lors que les données ne sont plus nécessaires pour la facturation, elles doivent être effacées ou anonymisées. De plus, seuls les collaborateurs et autres personnes ayant besoin des données pour l'accomplissement de leurs tâches doivent y avoir accès. Ces personnes doivent être formées et sensibilisées au droit de la protection des données. Enfin, il convient de garantir une gestion correcte des demandes de renseignements des personnes concernées, de façon à ce que ces dernières puissent obtenir des informations précises sur les traitements effectués et les données concernées.

1.3 Internet et télécommunication

1.3.1 Clôture de l'établissement des faits concernant Windows 10

Nous avons clos la procédure d'établissement des faits relative au système d'exploitation Windows 10 de Microsoft. L'entreprise a suivi nos recommandations concernant l'amélioration de la transparence du traitement des données et des possibilités de choix pour les personnes concernées.

Dans le cadre de la procédure d'établissement des faits relative au système d'exploitation Windows 10 qui a débuté en 2015 (cf. notre 23^e rapport d'activités 2015/2016, chiffre 1.3.1), nous avons constaté que le traitement des données dans Windows 10 n'était pas toujours conforme au droit sur la protection des données. Ainsi, la structure et le contenu des écrans «démarrer rapidement» et «paramètres de personnalisation» ne respectaient pas toutes les exigences de transparence de l'information. Aucune information n'était fournie au sujet de la durée d'archivage des données transmises et du contenu des données de navigation, ainsi que sur le contenu des rapports d'erreurs et de diagnostic. De plus, il n'était pas aisé pour les utilisateurs de consulter des informations détaillées sur les différents traitements de données, et notamment d'accéder aux passages correspondants de la déclaration de confidentialité. Nous avons donc émis plusieurs recommandations.

Microsoft nous a soumis des propositions afin de remédier aux défauts constatés. Nous avons pu prendre position à cet égard et nos avis ont été pris en compte par Microsoft, de sorte que nos recommandations ont été mises en œuvre conformément aux exigences de la protection des données, et une procédure devant le Tribunal administratif fédéral a pu ainsi être évitée. Les informations concernant les traitements de données sont désormais plus précises. De plus, le nouvel écran de personnalisation des paramètres qui s'affiche lors du processus d'installation indique clairement aux utilisateurs qu'ils doivent définir les traitements et transmissions de données dans le cadre de Windows 10 et les autoriser.

La mise en œuvre technique des adaptations que nous avons exigées aura lieu à l'échelle internationale dans le cadre des deux nouvelles versions de Windows 10 prévues en 2017. Dans la première version, des informations complètes concernant les possibilités de paramétrage des transmissions de données seront fournies aux utilisateurs lors de la première installation ou de la mise à jour du système d'exploitation. Dans la seconde version, les utilisateurs disposeront lors du

processus d'installation également d'un accès direct aux passages correspondants de la déclaration de confidentialité. L'intégration de liens vers des informations détaillées augmente la transparence et permet aux utilisateurs une meilleure compréhension de la déclaration des données.

Indépendamment de l'adaptation future du processus d'installation, les utilisateurs de Windows 10 ont la possibilité de modifier à tout moment les paramètres de traitement et de transmission des données.

Nous estimons que la solution trouvée, en particulier le lien vers les passages pertinents de la déclaration de confidentialité et les possibilités de paramétrage, constitue un standard minimal pour les applications et les services d'autres entreprises. Elle fera désormais office de référence lors de nos examens futurs pour le contrôle des traitements de données.

1.3.2 Nouvelles dispositions de Swisscom en matière de protection des données

Au cours de l'année sous revue, Swisscom nous a informés d'un projet de modification de ses traitements de données. Dans ce contexte, nous avons expliqué à l'entreprise ses obligations légales concernant l'information et le consentement des clients.

Au cours de l'année sous revue, Swisscom a planifié l'introduction de diverses modifications dans le traitement de ses données clients. L'objectif visé est de pouvoir transmettre aux clients des offres publicitaires sur mesure. Par ailleurs, certaines données ne permettant pas l'identification des personnes seront mises à disposition du réseau publicitaire Admeira. Swisscom a formulé l'intention d'informer sa clientèle dans une déclaration de protection des données séparée et d'adapter ses conditions générales en conséquence. Elle nous a demandé de prendre position sur ces projets.

Notre examen a révélé que l'extension prévue du traitement des données induisait l'établissement de profils de personnalité au sens de la loi sur la protection des données. Comme les données sont traitées dans un nouveau but (marketing), un motif justificatif est nécessaire. Dans le cas présent, seul le consentement de la personne concernée peut être envisagé. Selon la loi sur la protection des données, le traitement de profils de personnalité n'est autorisé que si la personne concernée y a explicitement consenti. L'entité qui traite les données est soumise à une obligation d'information

étendue: en recueillant le consentement écrit ou par voie électronique du client, elle doit informer ce dernier de façon concise de la création de profils de personnalité, sans quoi le consentement n'est pas valable. Cette information doit comprendre un renvoi aux points correspondants de la déclaration de protection des données, pour une consultation plus approfondie des informations.

Les clients ont le droit de refuser a posteriori le traitement de leurs données à des fins de marketing ainsi que la transmission des données à des tiers. L'entreprise doit veiller à ce que ce refus puisse être communiqué selon des modalités aussi simples que possible. Swisscom a proposé d'informer ses clients existants, par courrier individuel, des nouvelles conditions générales et de la déclaration de protection des données séparée. Ce courrier devait également expliquer très clairement comment les clients peuvent s'opposer au nouveau traitement des données. Nous avons approuvé cette proposition, qui répond aux impératifs d'information et de transparence. Pour les nouveaux clients, l'entreprise de télécommunication prépare actuellement une solution transparente pour intégrer la nouvelle déclaration de protection des données et le consentement explicite dans les variantes en ligne et hors ligne. Chaque client a en outre la possibilité de s'opposer au traitement de ses données personnelles à des fins de marketing, ou de révoquer son consentement, soit en ligne, dans son espace client, soit par téléphone.

Ces mesures, pour l'instant partiellement appliquées, respectent les exigences légales. Nous restons en contact avec Swisscom et allons accompagner la mise en œuvre définitive de nos suggestions.

1.3.3 Protocole Internet IPv6 et protection des données

Les adresses IP du protocole IPv4 actuel étant épuisées, l'introduction du nouveau protocole (version 6) est actuellement en cours. Par rapport à l'IPv4, le protocole IPv6 offre un certain nombre d'avantages pratiques, mais comporte également certains risques pour la protection des données et la sphère privée. Ces risques peuvent être minimisés grâce à des mesures techniques et organisationnelles adaptées.

Le protocole Internet définit les règles de base de la communication entre les ordinateurs et les appareils sur Internet. Le protocole IPv4 actuel, qui utilise des adresses courtes de 32 bits seulement, a atteint ses limites. C'est pourquoi un nouveau protocole, IPv6, a été développé. Outre l'élargissement des adresses à 128 bits, le protocole IPv6 offre également de nouvelles fonctionnalités utiles à la sécurité des données. Ce protocole autorise en principe la traçabilité des adresses IP, ce qui induit des risques en matière de protection des données qu'il importe de contrôler. Une attribution dynamique des adresses aux utilisateurs finaux (jusqu'à présent nécessaire du fait de la pénurie d'adresses) doit rester possible pour empêcher le traçage. Cependant, une traçabilité reste encore possible par l'intermédiaire de l'identifiant d'interface (Interface Identifier). Cet identifiant est identique à l'adresse matérielle fixe (MAC). Grâce à «Privacy Extensions», un processus d'anonymisation des adresses IPv6, il est possible, par la génération régulière de valeurs aléatoires, d'obtenir un «brouillage».

L'essentiel est qu'un internaute ne puisse pas être identifié à son insu par son adresse IP. L'identification doit pouvoir être reconnaissable et intentionnelle (p. ex. lorsque l'internaute se connecte à son compte e-mail ou de réseau social, ou lorsqu'il accepte des cookies).

Nous avons publié une fiche d'information concernant le protocole IPv6 ainsi qu'une liste de liens sur notre site Internet www.leprepose.ch, Protection des données – Internet et ordinateur.

1.4 Justice, Police, Sécurité

1.4.1 Loi sur l'identification électronique

Le projet de loi sur l'identification électronique contient une disposition adéquate de protection des données. Par contre, il est envisagé d'utiliser le numéro AVS en tant qu'identifiant personnel unique, ce à quoi nous nous sommes opposés.

L'Office fédéral de la justice a mis en consultation des offices un projet de Loi fédérale sur les moyens d'identification électronique reconnus par l'État (Loi e-ID). Le projet contient une disposition relative à la protection des données personnelles qui stipule que les fournisseurs d'identités électroniques reconnus ne peuvent traiter les données d'identification personnelles attestées par l'État que pour procéder aux identifications et aux authentifications. De plus, ils ne peuvent transmettre les données d'identification personnelle qu'aux parties utilisatrices qui offrent le niveau de garantie requis et à condition que le titulaire de l'e-ID y consente. La disposition prévoit également que les fournisseurs d'identité électronique et les parties utilisatrices ne peuvent faire le commerce des données d'identification personnelle attestées par l'État ou des profils d'utilisateurs établis sur la base de ces données.

Dans notre prise de position, nous avons rappelé notre opposition à l'utilisation du numéro AVS en tant qu'identificateur universel de personnes dans toute l'administration et en dehors. Nous avons également indiqué que les fournisseurs d'identité électronique accomplissent une tâche de la Confédération et qu'ils doivent être ainsi considérés comme des organes fédéraux en matière de protection des données. La consultation relative au projet de loi e-ID est prévue pour le premier semestre 2017. En ce qui concerne l'utilisation du numéro AVS, une nouvelle note de discussion à l'attention du Conseil fédéral est en préparation. Celle-ci conclurait à l'utilisation du numéro AVS en tant qu'identificateur universel de personnes dans les administrations fédérale, cantonales et communales.

1.4.2 Surveillance de la correspondance par poste et télécommunication – Révision totale des ordonnances du Conseil fédéral

Au cours de l'année sous revue, les ordonnances de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication ont été révisées. Lors de la consultation des offices, nous avons notamment pris position sur le droit d'accès aux données, la journalisation et la recherche par champ d'antennes.

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). Lors des séances en commission, nous avons exprimé notre compréhension pour les initiatives visant à prévoir un archivage des données accessoires en Suisse, bien que la loi sur la protection des données règle déjà l'externalisation de données personnelles à l'étranger. L'archivage de données accessoires en Suisse pourrait en l'occurrence réduire les risques d'accès aux données par des autorités étrangères.

Concernant les dispositions d'exécution, nous avons en particulier pris position sur le droit d'accès aux données, la journalisation, la recherche par champ d'antennes et les données accessoires dans le domaine de l'itinérance (roaming):

- Nous avons exigé que les détails du droit d'accès et du droit de consultation du dossier soient réglés dans l'ordonnance, comme cela est prévu dans la loi fédérale – en particulier la transmission des demandes d'accès et de consultation des dossiers à l'autorité ayant ordonné la surveillance.
- Concernant les procès-verbaux de journalisation des accès et traitements, le texte initial prévoyait un délai de conservation plus court que pour les données concernées, ce que nous avons jugé insatisfaisant. Les procès-verbaux ne peuvent remplir leur fonction de contrôle que s'ils sont disponibles pendant toute la durée d'archivage des données sur lesquelles ils portent. Aussi avons-nous exigé que la durée de conservation des procès-verbaux soit alignée sur celle des données correspondantes.
- Selon l'ordonnance, des recherches par champ d'antennes peuvent être demandées sur une durée maximale de deux heures pour une cellule d'antenne déterminée ou un point d'accès WLAN déterminé. Comme nous l'avions déjà exposé lors de la procédure de consultation concernant la loi fédérale, une recherche par champ d'antennes peut

conduire, en l'absence de critères de délimitation suffisamment restrictifs, à une recherche par quadrillage. Si les données de toutes les personnes présentes en un lieu donné à un moment donné sont transmises, cela peut aboutir à une atteinte disproportionnée aux droits fondamentaux de nombreux individus. Selon nous, les autorités de poursuite pénale doivent circonscrire leurs requêtes sur la base de critères de délimitation, ce qui réduit également la quantité de données à transmettre. Une solution envisageable consisterait à confier au Service Surveillance de la correspondance par poste et télécommunication la délimitation de la recherche, dans le cadre des informations sur les recherches par champ d'antennes standardisées.

- S'agissant des dispositions d'exécution concernant l'itinérance, les données que les prestataires suisses devaient transmettre n'étaient selon nous pas définies suffisamment clairement. Nous estimons que les fournisseurs de services de télécommunication en Suisse ne doivent transmettre que les données qu'ils recueillent ou qui leur sont transmises pour des raisons techniques liées à l'itinérance, ainsi que les données transmises par défaut pour la facturation. Aucune obligation plus étendue n'émane à notre avis de la loi. C'est pourquoi nous avons exigé la concrétisation de la disposition correspondante

Comme le contenu des ordonnances est très technique, nous avons proposé, pour en améliorer la compréhension, de publier également des explications concernant les différentes dispositions d'application.

1.4.3 Groupe de coordination des autorités suisses de protection des données dans le cadre de Schengen

Par le biais du «groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre de l'accord d'association à Schengen», nous coordonnons avec les autorités cantonales de protection des données nos activités de surveillance des traitements de données effectués en Suisse en matière de migration, police et justice en application de la coopération Schengen.

Le groupe de coordination des autorités suisses de protection des données s'est réuni deux fois au cours de l'année sous revue.

À l'occasion de la première réunion, un groupe de travail «contrôles coordonnés» a été créé. Ce dernier a pour objectif de revoir le concept de contrôle et d'élaborer un document à l'attention de toutes les autorités de protection des données suisses afin de faciliter les contrôles dans le domaine Schengen. Le groupe s'inspirera, entre autres, des documents d'audit récemment adopté par le groupe de coordination de contrôle du SIS II à Bruxelles.

Lors de la deuxième réunion, nous avons informé les autorités cantonales de protection des données des principaux points abordés par le groupe de coordination de contrôle du SIS II. Nous avons également informé nos collègues cantonaux des différents contrôles que nous allons mener et des débuts des travaux en vue de l'évaluation Schengen 2018. Les cantons quant à eux ont présenté les résultats de leurs activités de contrôle. Finalement, le groupe de travail «contrôles coordonnés» a présenté l'avancement de ses travaux.

1.5 Santé et recherche

1.5.1 Loi fédérale sur le dossier électronique du patient

Les dispositions d'exécution de la loi fédérale sur le dossier électronique du patient règlent, au niveau de l'ordonnance, de nombreuses prescriptions pertinentes en matière de protection et de sécurité des données. Les conditions de certification techniques et organisationnelles revêtent à cet égard une importance cruciale. L'entrée en vigueur de cette loi impliquera de nouvelles tâches pour notre autorité.

Au cours de l'année écoulée, l'Office fédéral de la santé publique (OFSP) a poursuivi les travaux consacrés aux bases légales du dossier électronique du patient. Après approbation par le Parlement de la loi fédérale sur le dossier électronique du patient (LDEP) et expiration du délai référendaire sans demande de référendum, les dispositions d'exécution prévues au niveau de l'ordonnance et les conditions de certification techniques et organisationnelles figuraient alors au programme. Mais il fallait encore à ce propos travailler sur de nombreuses prescriptions concrètes de protection des données; nous avons donc participé de manière intense à ces travaux dans le cadre de conférences, de réunions et de consultations des offices.

Notre préoccupation première était que ces prescriptions garantissent un niveau de protection maximum et que leur applicabilité soit assurée. A ce propos, nous avons dû faire quelques concessions. Par exemple l'affaiblissement, par les autorisations de groupe, du principe de l'autorisation individuelle des professionnels de santé pour l'accès au dossier électronique du patient. En revanche, nous avons obtenu que les patients puissent en tout temps reconstituer la composition du groupe de professionnels de santé. Pour nous, cette information était d'autant plus importante compte tenu du fait que, lorsqu'un nouveau professionnel de santé intègre un groupe, il bénéficie automatiquement des autorisations d'accès du groupe.

Dans le domaine des conditions de certification techniques et organisationnelles, nous considérons comme un pas important le fait que la grande majorité des données conservées par les communautés (regroupements de professionnels de la santé et de leurs institutions) doivent être cryptées. Le risque d'utilisation abusive de ces données par des attaquants externes s'en trouve largement réduit.

En outre, dans ce domaine, notre autorité devra assumer de nouvelles tâches, pour lesquelles elle a demandé au Conseil fédéral de ressources supplémentaires afin de pouvoir venir à bout avec les ressources en personnel dont elle dispose actuellement. Avec l'entrée

en vigueur de la LDEP, nous serons l'autorité compétente de surveillance de la protection des données pour les communautés de cybersanté et les éditeurs de moyens d'identification. Certes, l'OFSP interviendra ici en tant que propriétaire du schéma d'authentification et surveillera le respect des prescriptions de certification en collaboration avec les certificateurs, mais nous demeurerons l'autorité de surveillance compétente pour la protection des données et la sécurité des données. Nous ne savons pas encore quelle forme prendra la répartition concrète des tâches entre l'OFSP et notre autorité, et quel sera notre charge de travail. Mais la protection des données et la sécurité des données étant reconnues comme un facteur essentiel du succès du dossier électronique du patient, notre rôle en matière de contrôle et de conseil sera considérable..

1.5.2 Projet BAGSAN de l'Office fédéral de la santé publique

Sur la base de nos conseils, le projet BAGSAN a permis de prendre d'importantes mesures visant à garantir l'anonymat des assurés. BAGSAN montre clairement que, dans les projets impliquant de très grands volumes de données, il convient de surveiller en permanence le risque de ré-identification.

Selon le projet BAGSAN (statistique fondée sur les données des assurés), les assureurs-maladie devraient livrer chaque année, pour chaque personne assurée, plusieurs ensembles de données à l'Office fédéral de la santé publique (OFSP). Une procédure d'anonymisation garantit que cet Office reçoit pour chaque ensemble de données un identificateur qui fait le lien entre les ensembles de données sur plusieurs années de référence sans établir toutefois de rapport avec les personnes concernées. Ces données sont donc à la disposition de l'OFSP pour établir des statistiques très étendues et permettent d'améliorer le contrôle, la gestion et la planification dans le domaine de l'assurance-maladie.

Dans ce projet, nous avons souligné en particulier le fait que même s'il ne s'agit que de données utilisées dans le cadre précité, leur niveau de détail, leur caractère unique, leur accumulation et leur interconnexion peut permettre une réidentification. Plus généralement, dans un projet touchant un très grand volume de données (Big data ou mégadonnées), il convient de tenir compte de cette spécificité au moyen d'une procédure de surveillance fondée sur le risque. A ce sujet, nous avons eu une discussion approfondie avec l'OFSP dans le cadre de notre activité de conseil. L'Office a utilisé

une approche novatrice pour nous montrer les risques statistiques des réidentifications. Cette approche permet d'établir une estimation des risques aussi quant aux étapes ultérieures du projet et de maintenir au plus bas la probabilité d'une réidentification avec les moyens appropriés, par exemple la minimisation des données. Il est toutefois impossible d'éliminer totalement les risques. C'est pourquoi il est important que nous accompagnions aussi, tout au long des étapes à venir de ce projet, les mesures visant à garantir l'anonymat des personnes assurées.

1.5.3 Externalisation de la facturation dans le domaine médical

L'externalisation de la facturation dans le domaine médical n'est pas un phénomène nouveau. Depuis longtemps, des sociétés spécialisées s'occupent de l'établissement de factures et de leur encaissement. Malgré cela, certaines conditions en matière de transparence à l'égard des patients ne semblent pas encore suffisamment respectées. La situation est particulièrement délicate lorsque les prestataires utilisent les données des patients dans leur propre intérêt, par exemple pour créer une banque de données de solvabilité des patients ou leur notation.

La préoccupation première des professionnels de la santé, c'est le bien-être de leurs patients. On ne s'étonnera donc guère qu'ils confient volontiers la facturation et l'encaissement de leurs activités à des sociétés spécialisées. La pression croissante sur les coûts est certainement aussi une raison poussant les professionnels de la santé à externaliser au maximum leurs tâches administratives. Mais à ce propos, il convient de respecter un certain nombre de principes de protection des données, de dispositions cantonales et enfin, et surtout, le code pénal.

Dans le cadre d'une externalisation de la facturation, il est inévitable que des informations qui sont couvertes par le secret professionnel conformément au code pénal ou sont soumises à des dispositions cantonales de confidentialité soient communiquées au prestataire en question. Les données des patients tant administratives que médicales sont soumises à ces dispositions. Afin de ne pas transgresser ces prescriptions, la communication de ces données aux prestataires nécessite le consentement exprès du patient et pour des raisons de preuve, le consentement doit absolument être donné par écrit. L'examen critique portera ici en particulier sur les traitements de données, effectués par

ces prestataires, qui vont au-delà de la facturation et de l'encaissement proprement dits.

Ainsi nous avons constaté que certains prestataires utilisent une partie des données de facturation et d'encaissement pour alimenter leur propre base de données portant sur la solvabilité des patients par exemple ou pour établir une notation de ceux-ci, et entendent vendre également ces données à des tiers. Là aussi, la transparence doit prévaloir à l'égard du patient. Pour qu'une relation de soignant à soigné soit accompagnée par la confiance requise, il nous semble peu adéquat que le médecin doive encore expliquer au patient que ses données peuvent être utilisées par le prestataire chargé de l'établissement des factures pour les besoins propres de ce dernier, par exemple établir une évaluation du risque-client, et même les vendre à des tiers. Il est évident qu'on ne peut légitimer ce type d'utilisation des données par le prestataire en apposant simplement une information générale dans les locaux du cabinet médical. Même une telle mention, imprimée en petits caractères, sur le formulaire d'inscription dans lequel le patient donne d'ordinaire son consentement en vue de la transmission de ses données pour la facturation et l'encaissement, nous semble délicate.

En vertu des obligations légales concernant le secret médical, les professionnels de la santé se doivent d'être précis et d'attirer l'attention du patient clairement sur les traitements de données prévus effectués par le prestataire, y compris la vente possible à des tiers, et à recueillir le consentement exprès du patient. Cette méthode est aussi dans l'intérêt du prestataire. Indépendamment des chances de succès d'une plainte de droit civil déposée par un patient contre un prestataire pour violation de la personnalité, nous continuons à suivre de près les développements dans ce domaine et nous réservons expressément la possibilité de prendre des mesures.

1.6 Assurances

1.6.1 La libération du secret médical dans le cadre d'une procédure AI

L'échange des données concernant la santé des assurés dans le cadre d'une procédure AI va relativement loin. La situation est identique quant à la levée du secret médical. Dans le même temps, les principes généraux de protection des données posent des limites que les autorités se doivent de respecter.

Au cours de l'exercice écoulé, nous avons reçu de nombreuses reprises des questions de personnes impliquées dans une procédure AI conformément à la loi fédérale sur l'assurance-invalidité (LAI). Certains assurés étaient dans la phase de détection précoce des personnes en incapacité de travail. Pour d'autres, des mesures d'intervention précoce ou un examen de leurs prétentions pour une rente AI étaient en discussion ou bien la révision de leur rente était imminente.

Les questions posées par ces particuliers concernaient pratiquement toutes la licéité de l'échange de données personnelles, dans ce cas de données de santé, au sein d'une autorité et entre offices. En vertu de la loi sur la protection des données (LPD), les données de santé sont des données personnelles sensibles dont le traitement est soumis à des conditions très strictes. La question souvent posée a donc été celle de la portée de l'autorisation donnée par l'assuré, levant le secret professionnel à l'intérieur de l'autorité. Jusqu'où va cette autorisation? Tous les collaborateurs d'un service AI peuvent-ils consulter les dossiers du cas traité? À quels prestataires les dossiers d'une personne assurée peuvent-ils être envoyés lorsqu'il s'agit par exemple de l'examen du degré d'invalidité ou de la révision de la rente?

Il est vrai que la LAI et le règlement y relatif (RAI) sont des actes législatifs fédéraux. Mais la mise en œuvre de l'assurance-invalidité est du ressort des services cantonaux, c'est-à-dire des offices AI cantonaux, accompagnés de leurs services médicaux régionaux (SMR) et des caisses de compensation AVS. Sur les questions de droit de protection des données, ces services cantonaux ne sont pas soumis à notre surveillance et la LPD n'est pas applicable. En outre, c'est le préposé à la protection des données du canton dans lequel la procédure AI a lieu qui est compétent en matière de surveillance prévue par le droit de la protection des données. Tout en sachant que nous ne sommes donc pas compétents pour traiter ces cas précis, nous avons néanmoins fourni une brève analyse de la situation juridique aux particuliers qui nous avaient adressé une demande.

S'il est un échange qui peut aller relativement loin, c'est l'échange de données personnelles, en particulier de données de santé dans le cadre d'une procédure AI à l'intérieur d'un office AI et entre autorités. On peut le comprendre lorsqu'on considère la multitude des tâches que remplissent les offices AI. Ils sont par exemple chargés de la détection précoce des assurés en incapacité de travail et de l'intervention précoce visant à éviter une menace d'invalidité. En outre, les offices AI doivent examiner les conditions d'assurance, c'est-à-dire examiner la question de l'obligation de verser une prestation dans un cas concret. Pour ce faire, les offices AI ont aussi besoin des documents des caisses de compensation AVS et de leur collaboration au cours dudit examen. Par ailleurs, les offices AI sont compétents quant à l'examen de la capacité de réinsertion des personnes assurées, ordonnent les mesures de réinsertion et les contrôlent. Ils constatent le degré d'invalidité ainsi que le degré d'impotence et rendent des décisions sur les prestations de l'AI.

Pour accomplir leurs tâches, les offices cantonaux de l'AI peuvent recourir à toute une série d'autres services, par exemple les Centres d'observation médicaux de l'AI (COMAI) et les spécialistes chargés de l'examen de l'obligation du droit aux prestations de l'AI. Dans un tel contexte, les offices AI peuvent et doivent échanger ainsi que communiquer des données concernant la santé des assurés car ils sont tenus de clarifier chaque cas de manière approfondie. A cet effet, ils ont besoin des données les plus diverses qui peuvent fournir des renseignements sur les motifs médicaux et autres qui ont mené à une incapacité de travail de l'assuré en question. Si les offices AI n'étaient pas autorisés à traiter ces données personnelles et données de santé ainsi qu'à les transmettre à d'autres services, ils ne pourraient pas remplir les tâches qui leur incombent. Certes les règles de protection des données servent aussi les intérêts de l'assuré qui requiert des prestations de l'AI. Mais seules doivent être traitées, communiquées ou transmises les données qui sont nécessaires à l'appréciation du cas d'espèce et requises par le but poursuivi. Des limites sont ainsi posées, grâce aux principes de finalité et de proportionnalité, aux traitements de données effectués par les services intervenant dans la procédure de l'AI.

Il en va de même de la levée de l'obligation de garder le secret. À plusieurs reprises, nous avons reçu des demandes de personnes qui, dans le cadre de l'examen de leurs prétentions à des mesures de réinsertion AI ou à une rente, ont signé une autorisation d'octroi de renseignements. Ce faisant, elles avaient libéré différents offices et personnes de leur obligation de garder le secret (cf. art. 6a LAI). Cette autorisation ne vaut que pour ce

qui est nécessaire afin d'éclaircir la situation personnelle du requérant du point de vue médical, professionnel et social. Là aussi, les principes de finalité et de proportionnalité posent des limites aux traitements de données. On ne peut communiquer des renseignements et traiter ou fournir des documents que lorsque cela est nécessaire afin d'éclaircir le cas d'espèce. La consultation des documents doit être limitée aux personnes qui doivent les consulter compte tenu de la situation de fait. Néanmoins c'est l'assurance, et non pas l'assuré, qui détermine ce qui est nécessaire dans un cas précis.

1.6.2 Contrôle des services de réception de données des assureurs-maladie

Depuis le 1^{er} janvier 2014, chaque assureur-maladie doit disposer d'un service de réception des données (SRD) certifié pour la réception des factures de type «Diagnosis Related Groups» (DRG). Au cours de l'année sous revue, nous avons procédé à trois contrôles de ces services et avons pu constater un fonctionnement satisfaisant des SRD. Dans quelques cas, nous avons repéré des lacunes que nous avons notifiées au service de certification concerné.

Durant l'année sous revue, nous avons contrôlé trois SRD certifiés dans le cadre de procédures d'établissement des faits. Nos contrôles ont également porté sur les interfaces entre les différents acteurs, par exemple entre les intermédiaires et les SRD.

Lors de ces contrôles, nous avons généralement constaté les mêmes problèmes qu'au cours de l'année 2014/2015. Nous renvoyons à nos explications dans le 22^e rapport d'activités, chiffre 1.6.1).

Au cours de l'année sous revue, aucune séance de coordination n'a pu être organisée avec l'Office fédéral de la santé publique (OFSP). L'objectif des séances des années passées était de coordonner les activités de surveillance, partiellement redondantes, des deux autorités, et d'aborder des questions en suspens concernant les SRD et d'autres thèmes afférents.

Une séance a de nouveau eu lieu au cours de l'année sous revue avec les certificateurs des SRD et avec le service d'accréditation (SAS). Cette année encore, cette séance a été l'occasion de discussions constructives portant sur la certification, la mise en œuvre et la fonction des SRD, les interfaces entre les différents acteurs (hôpitaux, intermédiaires, etc.) et la clarification de certaines divergences d'opinion.

Dans l'ensemble, nous pouvons constater que la mise en œuvre de l'article 59a de l'ordonnance sur l'assurance-maladie continue à se dérouler de façon satisfaisante et globalement conforme à la loi. La collaboration avec les certificateurs, les assureurs et les exploitants de SRD électroniques a été constructive.

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

Les assureurs de véhicules à moteur disposent d'une base de données commune pour lutter contre la fraude. Ce modèle doit à présent être étendu à d'autres branches d'assurance. Nous avons émis des recommandations à ce sujet à l'intention du secteur des assurances.

Les assureurs de véhicules à moteur exploitent une plateforme électronique de données destinée à appuyer la lutte contre la fraude à l'assurance (Car Claims-Information). Un contrôle nous a permis de constater que le système était globalement conforme aux prescriptions en matière de protection des données (cf. 18^e rapport d'activités 2010/2011, chiffre 1.6.1). Des efforts sont actuellement déployés en vue de créer un pool de sinistres qui étendrait ce moyen de lutte contre la fraude à d'autres branches d'assurance.

En réponse à une demande de conseil, nous avons fait référence aux exigences actuelles en matière de protection des données. Nous avons rappelé en particulier que le but de la collecte de données devait être défini avec une précision suffisante et que le traitement des données devait être conforme au principe de la proportionnalité. Par ailleurs, les personnes concernées, en l'occurrence généralement les preneurs d'assurance, doivent être suffisamment informés, et une attention particulière doit être portée à l'exactitude des données.

1.6.4 Explications relatives aux capteurs fitness en lien avec les assurances

Parmi les nombreuses applications de fitness connectées avec des dispositifs que l'on porte sur soi (ou «wearables»: bracelets santé, smartwatches) contenant des capteurs d'activités, beaucoup n'offrent pas une protection suffisante des données. C'est pourquoi nous avons pris position concernant cette nouvelle technologie en publiant des explications détaillées sur notre site Internet.

S'amuser à mesurer ses propres paramètres corporels et performances au moyen d'applications de fitness ou de capteurs d'activités peut être motivant et s'avérer bénéfique pour la santé et le bien-être général. Cependant, en se mesurant ainsi, les utilisateurs produisent une quantité considérable de données numériques, qui deviennent rapidement difficiles à gérer. Le risque d'une perte de contrôle est bien réel et menace le droit fondamental à l'autodétermination informationnelle.

Les données qui renseignent sur notre état de santé ou nos maladies sont qualifiées de particulièrement sensibles par la loi sur la protection des données (LPD), car leur transmission et leur traitement constituent une intrusion massive dans la sphère privée. En utilisant des capteurs ou traqueurs fitness, nous révélons non seulement des informations très diverses sur notre santé, mais créons également un profil révélateur de notre personnalité. Les données ainsi générées présentent un intérêt notable pour les acteurs du domaine de la santé, mais aussi pour d'autres secteurs économiques. Le fait que des tiers puissent avoir accès à des informations relatives à la santé des individus et les utiliser à des fins contraires à l'intérêt des personnes concernées peut avoir des effets néfastes majeurs.

Conscients de la popularité croissante de ces technologies, les assureurs-maladies sont de plus en plus nombreux à proposer des rabais sur les primes aux assurés qui sont disposés à mesurer leurs paramètres corporels et à leur transmettre ces informations. Or, cela pose un problème notable: des données relatives à la masse grasseuse, au sommeil, à la fréquence cardiaque et respiratoire peuvent permettre de tirer des conclusions sur l'état de santé et la présence d'éventuelles maladies, ce qui peut jouer en défaveur de la personne concernée (p. ex. augmentation des primes ou exclusion de certains risques lors de la conclusion de l'assurance).

Par ailleurs, lorsque les assureurs-maladie disposent de données relatives à la santé, ces informations personnelles risquent aussi d'être utilisées à d'autres fins. Dans ce contexte, le principe de transparence notamment doit être impérativement respecté (art. 4 LPD). Le traitement de données personnelles sensibles

requiert un consentement explicite des personnes concernées, lequel doit être donné librement, en l'absence de toute pression (en l'occurrence financière). De telles offres sont envisageables dans le domaine des assurances complémentaires facultatives, mais pas dans celui de l'assurance obligatoire des soins.

Nous avons publié sur notre site Internet des explications relatives aux capteurs fitness en lien avec les assurances (www.leprepose.ch, Protection des données – Santé – Assurance-maladie/accidents). Les citoyens y trouveront également des conseils utiles concernant l'utilisation de ces capteurs fitness.

1.7 Secteur de travail

1.7.1 Établissement des faits concernant la gestion électronique du recrutement et les dossiers de candidature dans l'administration fédérale

Au cours de l'année sous revue, nous avons contrôlé les traitements de données effectués dans le cadre du processus de candidature auprès de l'administration fédérale. Notre établissement des faits a révélé que les données personnelles des candidats faisaient l'objet d'un traitement conforme à la protection des données, à quelques exceptions près, tant dans le système de gestion électronique du recrutement que sur papier.

Pour avoir une vue d'ensemble des traitements effectués par les services fédéraux dans le cadre du processus de recrutement, nous avons sélectionné un service par département, que nous avons ensuite soumis à un examen approfondi. Pour la sélection des services, nous nous sommes fondés sur leur taille et sur le nombre d'offres d'emplois publiées.

Après une analyse de la documentation et des réponses demandées, nous avons procédé à des inspections sur place. Sur la base des observations effectuées, nous avons envoyé à tous les services une constatation des faits et un rapport final. Dans nos rapports finaux, nous avons affirmé que le traitement des données dans le cadre du système de gestion électronique du recrutement s'opérait de façon globalement conforme à la protection des données. Nous avons identifié des possibilités d'amélioration, notamment dans le contrôle des autorisations d'accès et dans le règlement de la gestion des dossiers papier. Après avoir communiqué ces suggestions aux services concernés, nous avons clôturé nos examens.

Pour un service, nous avons émis une recommandation. Nous lui avons demandé de supprimer certaines données de candidats, car leur conservation n'était pas conforme au principe de proportionnalité, et parce qu'il n'existe aucune base légale pour un tel archivage. Le service concerné a rejeté notre recommandation et l'a transmise au département compétent.

Comme l'Office fédéral du personnel (OFPER) est responsable du système de gestion électronique du recrutement, nous avons étendu nos examens à cet office. Au cours de deux réunions, nous avons examiné diverses possibilités d'amélioration, par exemple la possibilité pour le candidat de supprimer son propre dossier. L'OFPER procédera dans le système aux adaptations des points que nous avons critiqués. Nous vérifierons lors d'un contrôle ultérieur que ces améliorations ont bien été introduites.

1.8 Économie et commerce

1.8.1 Privacy Shield entre la Suisse et les États-Unis

En janvier 2017, le Conseil fédéral a pris bonne note de la mise en place d'un nouveau cadre de transmission des données personnelles de la Suisse vers les États-Unis. Ce cadre, baptisé «Privacy Shield», remplace le «Safe Harbor» conclu entre la Suisse et les États-Unis, jugé insuffisant par le PFPDT et officiellement invalidé par le Conseil fédéral. Nous avons joué un rôle consultatif dans les négociations qui ont mené à cet accord.

Dans notre 23^e rapport d'activités 2015/2016 (chiffre 1.8.1), nous avons traité de l'arrêt de la Cour de justice de l'Union européenne sur l'accord Safe Harbor et de ses conséquences pour la Suisse. En janvier 2016, nous avons adapté notre liste des États et constaté que la transmission de données vers les États-Unis ne pouvait s'appuyer sur le seul dispositif Safe Harbor. Des mesures supplémentaires de nature contractuelle étaient nécessaires pour garantir la conformité de cette transmission au droit de la protection des données.

En conséquence, le Conseil fédéral a chargé le Secrétariat d'État à l'économie (SECO) de constituer un groupe de travail interdépartemental ayant pour mission de négocier un nouvel accord pour remplacer le Safe Harbor. Nous avons participé aux séances de ce groupe de travail en qualité d'experts et avons suivi de près les négociations. Le Privacy Shield (bouclier de protection) entre l'Union européenne et les États-Unis est entré en vigueur en août 2016. Depuis lors, quelques centaines d'entreprises ont obtenu une certification sur la base de ce règlement. Concernant le Privacy Shield Suisse – États-Unis, nous avons exigé qu'il offre aux personnes concernées des garanties au moins équivalentes à celles prévues dans l'accord passé avec l'Union européenne. Les négociations avec les États-Unis ont permis d'atteindre cet objectif. Le Privacy Shield garantit une meilleure protection que Safe Harbor, grâce à un renforcement de l'application des principes de protection des données pour les entreprises certifiées et par une amélioration de l'administration et de la surveillance par les autorités américaines. Les mesures suivantes ont notamment été prises:

- Les autorités américaines mettront à disposition des personnes concernées des formulaires de contact sur le site internet dédié au Privacy Shield Suisse – États-Unis pour toute question relative à la protection des données. En plus de la liste des entreprises certifiées, une liste des entreprises qui ne sont plus certifiées y sera également publiée.
- La surveillance exercée par les autorités américaines sur les entreprises certifiées est renforcée.
- Les personnes concernées auront la possibilité, après recours à un mécanisme indépendant de règlement des différends, de s'adresser à un tribunal d'arbitrage régi par le droit américain pour s'opposer à des traitements de données portant atteinte à leur personnalité.
- Le Privacy Shield Suisse – États-Unis sera soumis chaque année à une procédure de réexamen, à laquelle participeront le SECO, les autorités de surveillance américaines et nous-même. Le SECO établira un rapport à l'attention du Conseil fédéral et nous consignerons de notre côté nos observations, en tirant nos propres conclusions.

La surveillance des autorités américaines de sécurité sera également renforcée. Un dispositif de médiation avec les instances de sécurité sera mis en place. Sur requête des citoyens concernés, le médiateur contrôlera que les données sont traitées correctement. Les personnes déposant une demande d'accès seront informées que leurs données sont traitées de façon conforme à la loi ou que la conformité à la loi a été rétablie.

Nous entendons à présent nous concentrer sur la mise en œuvre du Privacy Shield Suisse – États-Unis dans la pratique.

1.8.2 Agence de renseignements économiques et de crédit Moneyhouse – Action auprès du Tribunal administratif fédéral

Dans le cadre de la procédure engagée contre la société d'informations sur la solvabilité Moneyhouse, le Tribunal administratif fédéral a rendu une décision déterminante dans le contexte actuel de la numérisation, en imposant des limites claires à la mise en relation d'informations permettant l'établissement de profils ainsi qu'à leur publication.

Dans le cadre de son offre en ligne d'informations relatives à la solvabilité, la société d'informations sur la solvabilité Moneyhouse donne accès à des informations reliées de manière systématique qui contiennent notamment des données sur l'âge, la profession, le domicile et les cohabitants de particuliers. Face aux nombreuses protestations à cet égard, notre autorité a mené un examen des faits officiel, au terme duquel il a déposé plainte auprès du Tribunal administratif fédéral en vue de l'application de ses recommandations, contestées par Moneyhouse (cf. chiffre 1.8.5 de notre 23^e rapport d'activités 2015/16).

Dans son jugement du 18 avril, précédé dans l'année sous revue par plusieurs audiences et une procédure probatoire approfondie avec inspection, le tribunal établit que les données personnelles tirées de différentes sources ne peuvent être enregistrées, reliées et reproduites de manière illimitée. Il établit en outre que le respect de la sphère privée s'applique également à la société numérisée lorsqu'il s'agit, comme dans le cas présent, du traitement d'informations permettant de tirer des déductions sur le lieu de résidence et la situation personnelle, et donnant lieu à l'élaboration de profils de personnalité.

Conformément aux demandes du PFPDT, la société défenderesse est ordonnée à supprimer différents liens et données qui ne sont pas pertinents en matière de solvabilité et ne font l'objet d'aucun accord de la part des personnes concernées. En outre, Moneyhouse est tenu de prendre des mesures appropriées afin de garantir l'exactitude du contenu des informations sur la solvabilité. Ces informations ne doivent être transmises qu'aux clients qui disposent d'un intérêt légitime.

Au moment de l'impression on ne savait pas encore si la défenderesse porterait l'affaire devant le Tribunal fédéral.

1.8.3 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 metering).

Dans le cadre de la procédure de consultation sur les ordonnances relatives au premier train de mesures de la Stratégie énergétique 2050 du Conseil fédéral, 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. sur le thème de la publication: 23^e rapport d'activités 2015/2016, chiffre 1.2.6, et sur le thème des compteurs intelligents: 23^e rapport d'activités 2015/2016, chiffre 1.8.2).

Selon nous, le principe de proportionnalité revêt une importance primordiale lors de la publication de données personnelles sur Internet. Dans les projets de loi, la publication de données personnelles doit être adaptée à l'objectif. L'Office fédéral de l'énergie (OFEN) a à nouveau signalé son 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 est d'assurer la transparence concernant l'utilisation du supplément facturé aux consommateurs finaux.

Le gain de transparence résultant de la publication des données personnelles de producteurs percevant des rétributions de petits montants est discutable. L'atteinte au droit à l'autodétermination informationnelle de 5000 producteurs supplémentaires, qui ne représentent qu'environ 8 pour cent du montant total des rétributions, apparaît disproportionnée. Aussi avons-nous demandé que l'on renonce à l'élargissement de la publication sur Internet à tous les bénéficiaires de rétributions uniques et de RPC, d'autant plus que l'accès aux données sur ces bénéficiaires, indépendamment de la puissance de raccordement ou du montant de la rétribution, reste ouvert à tout citoyen qui en fait la demande selon les dispositions de la loi sur la transparence.

Concernant les dispositions d'exécution sur les compteurs intelligents, nous nous sommes prononcés sur l'accès des personnes concernées à leurs propres données, sur la pseudonymisation des données, sur la durée de conservation des valeurs de courbe de charge détaillées ainsi que sur la fréquence de consultation des

données. Du point de vue de la protection des données, ces thèmes avaient déjà été considérés comme essentiels lors du précédent processus législatif. Nous avons exigé que les personnes concernées aient la possibilité d'accéder à leurs données, y compris aux valeurs de courbe de charge, même à partir d'une interface standard, et de les exporter vers leur propre système ou le système de leur choix.

L'ordonnance prévoit également d'autoriser les gestionnaires de réseau à traiter les données enregistrées par les systèmes de mesure, de commande et de réglage intelligents sans l'autorisation des personnes concernées lorsque ces données servent aux commandes et aux réglages, ou lorsque leur utilisation est prévue pour l'application des systèmes tarifaires ainsi que pour une gestion sûre et efficace du réseau et la planification du réseau, sous forme pseudonymisée. Sous forme non pseudonymisée, les données ne peuvent être traitées que pour le décompte de la livraison énergétique, de la rémunération pour l'utilisation du réseau et de la rétribution de l'accès aux systèmes de commande et de réglage. Ces traitements incluent également les valeurs de courbe de charge selon une périodicité de quinze minutes et plus.

Les dispositions et les explications n'indiquent pas suffisamment clairement comment les gestionnaires de réseau doivent mettre en œuvre la pseudonymisation. Selon nous, il conviendrait au minimum d'appliquer le Guide du PFPDT relatif aux mesures techniques et organisationnelles de la protection des données (www.leprepose.ch, Protection des données – Documentation – Guides). Il importe notamment de veiller à ce que les données attribuées au pseudonyme ne puissent pas être reliées à une personne en particulier. Cela implique qu'aucune information permettant d'identifier indirectement une personne ne doit être transmise, et qu'il importe de choisir des identifiants «non parlants».

De plus, nous avons indiqué que, selon nous, tous les buts de traitement énoncés dans l'ordonnance ne nécessitaient pas des valeurs de courbe de charge de quinze minutes, ni leur conservation pendant douze mois. Nous estimons que certains buts peuvent tout aussi bien être atteints avec des données agrégées ou anonymisées. C'est pourquoi nous avons demandé qu'une durée maximale de conservation des profils de charge soit imposée, et qu'ils soient anonymisés ou agrégés le plus rapidement possible.

Enfin, nous avons exigé la réglementation de la fréquence de consultation des données enregistrées par les compteurs intelligents ainsi que des conditions pour leur consultation en temps réel, comme l'OFEN l'avait initialement prévu. Ces deux facteurs ont en effet une incidence décisive sur l'intensité de l'intrusion dans la sphère privée.

1.9 Finances

1.9.1 Communication de données personnelles à des autorités fiscales étrangères

La mise en œuvre des nouvelles normes pour la lutte internationale contre la fraude fiscale et l'évasion fiscale est déjà bien engagée. Dans le domaine de l'échange automatique de renseignements nouvellement instauré, la Suisse doit commencer en 2017 à collecter des données qui seront échangées pour la première fois en 2018. Nous avons pris position sur plusieurs projets de loi sous l'angle du droit de la protection des données.

En signant en 2013 la Convention de l'Organisation de coopération et de développement économiques (OCDE) et du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale, la Suisse s'est engagée à fournir une assistance administrative en matière fiscale (cf. 23^e rapport d'activités, chiffre 1.9.2.a). La Convention est entrée en vigueur le 1^{er} janvier 2017. Elle crée une base multinationale légitimant l'échange automatique et spontané de données fiscales à l'échelle internationale, qui doit être soumise à un examen critique au regard du droit sur la protection des données. La mise en œuvre de la Convention implique l'élaboration et la modification de diverses bases législatives. Notre tâche était et reste de garantir dans ce contexte le respect des exigences de la LPD.

Les différentes formes d'assistance administrative sont réglementées dans plusieurs lois. Au cours de l'année sous revue, nos prises de position ont porté en particulier sur l'échange automatique, mais aussi spontané, de renseignements.

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 doit commencer en 2017 à collecter des données qui seront 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), qui se fonde lui-même sur la Convention (cf. 23^e rapport d'activités 2015/2016, chiffre 1.9.2.c).

Par cette procédure d'activation, les États participants s'engagent à intégrer et à appliquer dans leur législation nationale la «norme commune de déclaration et de diligence raisonnable» de l'OCDE (norme commune de déclaration ou Common Reporting Standard, CRS). Elle régit l'échange mutuel de données sur les comptes et les dépôts de titres de contribuables entre les autorités fiscales des pays participants.

Ordonnance sur l'échange international automatique de renseignements en matière fiscale

Dans notre dernier rapport d'activités, nous évoquions la promulgation de la loi fédérale sur l'échange international automatique de renseignements en matière fiscale (LEAR) (cf. 23^e rapport d'activités 2015/2016, chiffre 1.9.2.b). Elle vise la mise en œuvre des conventions internationales et des normes EAR en Suisse. L'ordonnance sur l'échange international automatique de renseignements en matière fiscale (OEAR), adoptée par le Conseil fédéral fin 2016, concrétise cette législation. Elle entre en vigueur le 1^{er} janvier 2017.

Lors de la procédure de consultation sur l'adoption de l'OEAR, nous avons d'une part obtenu que la mise en réseau des systèmes d'information de l'Administration fédérale des contributions (AFC) soit limitée au but de la gestion des données de base. D'autre part, notre recommandation de maintenir dans l'ordonnance une réglementation du degré d'authentification a été suivie. Cette réglementation concerne la procédure d'appel des autorités cantonales aux informations reçues de l'étranger.

Par ailleurs nous sommes d'avis que la durée d'archivage de vingt ans avant la destruction des données est disproportionnée. Cependant, notre proposition de limiter la conservation des données à dix ans a été rejetée, et ce point a figuré parmi les divergences exprimées à l'intention du Conseil fédéral. Enfin, notre souci de régler également la transmission automatique d'informations vers l'étranger dans l'ordonnance n'a pas non plus été pris en compte. La raison invoquée par l'AFC est que l'intégration d'une réglementation dans l'ordonnance ne serait à l'heure actuelle ni possible, ni judicieuse. Du côté de l'OCDE, les spécifications pour l'intégration au système commun de transmission de l'Organisation ne sont pas encore connues, et la spécification technique de l'interface avec les cantons est encore en cours d'élaboration. Nous aurons toutefois la possibilité de prendre position sur le concept de sécurité et le règlement de traitement des données lors de l'annonce des fichiers.

Directive – Norme commune de déclaration

Dans la pratique, l'introduction et la mise en œuvre quotidienne de l'échange automatique de renseignements va confronter le secteur financier suisse à des questions épineuses. C'est pourquoi l'AFC a élaboré une norme pour l'échange automatique de renseignements relatifs aux comptes financiers. Ce texte, qui prend la forme d'une directive, décrit concrètement les obligations émanant des bases juridiques suisses régissant la mise en œuvre de la norme EAR pour les institutions financières suisses et les autres parties prenantes, notamment l'AFC.

Lors de notre prise de position sur la version provisoire, nous avons rappelé, concernant les données devant être traitées, les principes de la proportionnalité (les identifiants du bâtiment, de l'étage ou de l'appartement ne sont généralement pas utilisés en Suisse pour définir une adresse) et de l'exactitude des données (la date de naissance est nécessaire pour l'identification univoque d'une personne). De plus, nous avons attiré l'attention sur le risque de signaler par erreur une personne ne devant pas faire l'objet d'une déclaration dès lors que l'identification repose sur des informations publiquement accessibles, de qualité insatisfaisante ou méconnue.

Enfin, nous avons estimé qu'une information unique des clients était insuffisante et nous sommes prononcés en faveur de la publication d'informations générales, p. ex. sur le site internet de l'institution financière, en plus de l'information individuelle des clients concernés. Globalement, toutefois, la directive est, dans sa forme actuelle, conforme au droit de la protection des données et offre selon nous un moyen d'aide efficace pour l'évaluation des personnes devant faire l'objet d'une déclaration dans le respect des droits de la personnalité.

Exigences supplémentaires de la Suisse à l'égard d'États présentant un niveau insuffisant de protection des données

Nos efforts répétés pour faire valoir la nécessité d'exigences supplémentaires à l'égard d'États présentant un niveau insuffisant de protection des données ont porté leurs fruits: une communication concernant les exigences supplémentaires de la Suisse dans le domaine de la protection des données doit compléter l'EAR avec les États appliquant un niveau de protection des données inadéquat. Cette initiative va dans le bon sens, et nous la saluons. Toutefois, lors de la consultation des offices, nous avons pris position sur le contenu de la communication qui, selon nous, ne va pas assez loin.

Nous avons préconisé de limiter exclusivement l'utilisation des données aux buts de l'EAR et de pros-

crire toute utilisation portant atteinte aux droits fondamentaux et aux libertés individuelles. Nous reconnaissons toutefois que le texte exclut déjà explicitement toute violation grave des droits de l'homme. En outre, nous avons recommandé un élargissement du droit de recours, un devoir d'information situationnel et une interdiction explicite de la rétroactivité. Les résultats de la procédure de consultation n'étaient pas encore disponibles au moment de la rédaction du présent rapport.

Nouveaux arrêtés fédéraux sur l'introduction de l'échange automatique de renseignements avec plusieurs États

Quel que soit le type d'activation choisi pour l'EAR, l'arrêté fédéral ou l'accord bilatéral est soumis à l'approbation du Parlement. Au cours de l'année sous revue, le Parlement a approuvé l'introduction de l'EAR avec les pays suivants: Australie, Guernesey, Île de Man, Islande, Japon, Jersey, Canada, Norvège, Corée du Sud, ainsi que tous les États de l'UE, y compris Gibraltar (concernant l'Australie et l'UE, cf. également notre 23^e rapport d'activités 2015/2016, chiffre 1.9.2.). Fin 2016, le Parlement a également approuvé l'arrêté fédéral portant approbation de l'accord entre la Suisse et le Brésil sur l'échange de renseignements en matière fiscale. Dans le cadre des accords passés avec ces États, la collecte de renseignements débute au 1^{er} janvier 2017, et les données seront échangées à partir du 1^{er} janvier 2018.

L'EAR a été introduit avec une nouvelle série d'États et entrera en vigueur un an plus tard, si bien que les premiers échanges de données auront lieu sur cette base en 2019. Sont notamment concernés l'Argentine, les Bermudes, les Îles Caïman, l'Inde, Israël et le Mexique. Pour ces États, la consultation pour l'introduction de l'EAR s'est achevée le 15 mars 2017. Actuellement, la consultation pour l'introduction de l'EAR avec une deuxième série d'États est en cours, notamment la Chine, la Russie, l'Arabie saoudite, le Liechtenstein et les Émirats arabes unis, et elle doit s'achever le 13 avril 2017. Les deux projets seront ensuite réunis et présentés ensemble au Parlement, ce qui explique que la décision du Parlement n'ait pas encore été rendue au moment de la publication du présent rapport. Enfin, le 1^{er} janvier 2018, l'EAR sera également introduit avec Singapour.

Dans le cadre de la consultation des offices au cours de l'année sous revue, nous avons mis en avant l'exigence de garantie d'un niveau adéquat de protection des données dans les différents États partenaires. Notre liste de pays comprend des indications à ce sujet État par État. Dans tous les cas, nous avons mis en avant le cas des États pour lesquels nous n'avons pas connaissance d'une garantie de niveau adéquat

de protection des données. Nous sommes critiques à l'égard de l'application même de dispositions de protection des données convenues dans les instruments internationaux, dès lors qu'il n'existe pas, dans l'État partenaire, de conscience des risques d'atteinte à la personnalité induits par les traitements de données ni de dispositions adéquates pour prévenir ces risques. Le DFF a pour sa part estimé que les législations nationales existantes en matière de protection des données et/ou les prescriptions de protection des données convenues dans les instruments internationaux étaient suffisantes pour la mise en œuvre de l'EAR.

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 combattre l'optimisation fiscale de groupes multinationaux par l'échange automatique des déclarations pays par pays (EDPP). Ce projet s'appuie sur le projet commun «Base Erosion and Profit Shifting» (BEPS) de l'OCDE et des États du G20, qui s'attaque aux pratiques visant la double non-imposition par l'érosion de la base d'imposition et le transfert de bénéfices.

Les sociétés mères des groupes multinationaux sont tenues d'établir des déclarations pays par pays sur leurs bénéfices, leurs impôts et leurs activités. Ces rapports sont automatiquement transmis aux autorités fiscales nationales des États et territoires dans lesquels les groupes multinationaux exercent des activités. Toute entreprise active à l'international s'engage à procéder à ces déclarations pays par pays à partir d'un certain niveau de revenu annuel consolidé pour le groupe. En Suisse, environ 200 groupes devraient dépasser cette valeur seuil.

Début 2016, la Suisse a signé l'accord multilatéral portant sur l'échange des déclarations pays par pays (accord EDPP). Pour sa mise en œuvre, la loi fédérale sur l'échange international automatique des déclarations pays par pays des groupes d'entreprises multinationales (LEDPP) a été créée. Dans le cadre de la consultation des offices, nous avons pris position sur le projet de loi et insisté en particulier sur le fait que, conformément aux principes de transparence et de précision de la base légale, les données personnelles concrètement traitées devaient être énumérées dans la loi, laquelle devait également comprendre une liste exhaustive des finalités d'utilisation des systèmes d'information. De plus, nous nous sommes exprimés au sujet de la transmission et de l'utilisation des déclarations pays par pays, ainsi que sur la confidentialité.

Abrogation des accords sur l'imposition à la source avec l'Autriche et le Royaume-Uni

Du fait de l'entrée en vigueur de l'accord entre la Suisse et l'UE sur l'introduction de l'échange automatique de renseignements sur les comptes financiers, les accords sur l'imposition à la source avec l'Autriche et le Royaume-Uni n'ont plus de raison d'être. Le Conseil fédéral a donc conclu un accord d'abrogation avec ces deux États, pour faciliter le passage du système d'imposition à la source à l'EAR. Nos préoccupations concernant une réglementation insuffisante de la délicate question des demandes groupées ont trouvé des réponses.

b) Échange spontané d'informations – Modification de la loi sur l'assistance administrative fiscale et révision totale de l'ordonnance y relative

Avec l'adhésion à la Convention concernant l'assistance administrative mutuelle en matière fiscale, la Suisse a introduit également l'échange spontané de renseignements en matière fiscale. Dans ce cas, les renseignements sont communiqués sans requête préalable, lorsque l'État transmetteur présume, en se fondant sur les informations dont il dispose, que les renseignements sont susceptibles d'intéresser un autre État. Les dispositions d'exécution, la loi sur l'assistance administrative internationale en matière fiscale (LAAF) et l'ordonnance sur l'assistance administrative internationale en matière fiscale (OAAF) sont entrées en vigueur en même temps que la Convention concernant l'assistance administrative mutuelle en matière fiscale, le 1^{er} janvier 2017. La modification de la LAAF et la révision totale de l'OAAF ont fait l'objet d'une consultation des offices. Concernant la modification de la LAAF, nous avons déjà pris position dans le rapport d'activités 2015/2016, chiffre 1.9.2, et dans le rapport d'activités 2013/2014, chiffre 1.9.3.

Dans le cadre de la dernière procédure de consultation, nous avons recommandé divers ajustements concernant la formulation de la LAAF: Dans une première étape, nous avons souligné que la forme juridique des unités organisationnelles en charge de l'échange spontané de renseignements devait être plus précisément définie. Ce point est important pour déterminer si c'est la LPD ou une loi cantonale sur la protection des données qui s'applique, et quel organe de surveillance est compétent.

Dans une deuxième étape, nous avons indiqué que, en vertu des principes de proportionnalité et de finalité applicables à la protection des données, il convenait tout d'abord de vérifier, pour chaque État destinataire de renseignements, s'il s'agissait bien de l'État compétent pour l'imposition. Ensuite, nous avons recommandé de contrôler, pour chaque transmission optionnelle

de renseignements, si cette transmission était effectivement nécessaire pour l'imposition. Ces points ont donné lieu à des adaptations dans les explications.

Nous n'étions pas d'accord avec la possibilité octroyée à l'AFC de limiter la transmission aux États qui reconnaissent la norme de l'OCDE concernant l'échange spontané de renseignements sur les décisions anticipées, car la formulation contredit le principe de précision de la base légale. L'objectif premier de l'AFC est d'échanger avec tous les États. Ainsi, la formulation de la LAAF va dans la mauvaise direction. L'échange de données ne doit pas être conditionné uniquement au fait que l'autre État est également disposé à transmettre des données, mais aussi au niveau de protection des données qu'offre cet État.

1.10 International

1.10.1 Coopération internationale

L'année écoulée a été marquée par l'adoption de la réforme du cadre juridique de protection des données au sein de l'Union européenne. Elle a également permis de finaliser la modernisation de la Convention du Conseil de l'Europe au niveau des experts gouvernementaux. Ces textes sont au centre des réformes du droit européen et national de la protection des données. Dans le cadre de ses activités de coopération internationale, le PFPDT s'implique en particulier dans les travaux du Conseil de l'Europe, de l'Union européenne dans le cadre des accords de Schengen, des conférences européenne et internationale des commissaires à la protection des données et de l'Association francophone des autorités de protection des données.

Conseil de l'Europe

Les travaux de modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) se sont achevés au niveau des experts gouvernementaux qui ont adopté un projet de révision en juin 2016 (voir nos précédents rapports d'activités). Le Comité des Ministres du Conseil devrait adopter un protocole d'amendement à la Convention durant le premier semestre 2017. Avec la ratification par la Turquie de la Convention, tous les États membres du Conseil de l'Europe sont désormais parties à cet instrument. En outre, après l'Uruguay en 2013, l'Île Maurice et le Sénégal ont accédé à la Convention. D'autres États devraient y adhérer cette année.

La Comité consultatif de la Convention 108 (T-PD) a poursuivi ses travaux en vue de la révision de la recommandation R (97) 5 relative à la protection des données médicales, ainsi que ceux relatifs à la rédaction d'un guide pratique concernant la protection des données dans le secteur de la police. Il a en outre adopté un avis sur les implications en matière de protection des données du traitement des données passagers (données PNR). Dans cet avis, le comité conclut que compte tenu du risque d'atteinte particulière aux droits à la protection des données et à la vie privée, un système PNR doit strictement respecter les principes de légalité, de proportionnalité et de nécessité. Cela suppose notamment:

- une démonstration transparente et mesurable de la nécessité et de la proportionnalité du système au regard du but légitime poursuivi;
- des définitions précises et strictes de l'objectif légitime poursuivi sont nécessaires et le traitement des données PNR ne doit être autorisé que pour des motifs limités et bien définis (prévention, détection, instruction et poursuite des infractions de terrorisme et autres infractions graves, ou dans des cas exceptionnels, prévention de menaces graves au public);
- ne liste publique des autorités publiques compétentes (dans l'idéal, des unités de coordination spéciales);
- l'utilisation du «mode push» pour transmettre des données ainsi qu'une définition claire de la période de conservation initiale et des mesures de sécurité appropriées;
- une interdiction de l'utilisation systématique des données sensibles;
- une exploration des données limitée par des indicateurs de risque prédéfinis, avec un examen au cas par cas de la pertinence des résultats d'une manière non automatique;
- des limitations uniquement nécessaires et prévues par la loi aux droits d'information, d'accès, de rectification et d'effacement dont jouissent les individus;
- la compétence des autorités chargées de la protection des données (pouvant être consultées et habilitées à évaluer le système PNR et à traiter les plaintes individuelles);
- a disponibilité de voies de recours administratives et judiciaires effectives pour les personnes concernées; un contrôle externe indépendant du système PNR;
- un examen régulier du système PNR par les autorités compétentes.

Le comité a enfin poursuivi l'examen d'un projet de 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 qui seront adoptées prochainement par le comité définissent un cadre général afin de permettre aux Parties à la Convention de concevoir des politiques et des mesures de nature à rendre effectifs les principes et les dispositions de la Convention 108 dans le contexte des mégadonnées. Ce texte se veut évolutif et énonce des orientations générales qui pourront être complétées dans des domaines d'application spécifiques des mégadonnées.

Conférence européenne des commissaires à la protection des données

La conférence européenne des commissaires à la protection des données s'est déroulée en 2016 à Budapest à l'invitation de l'autorité hongroise de protection des données. Elle réunissait une centaine d'experts et de représentants des autorités de protection des données provenant de toute l'Europe. La conférence a mis l'accent sur les réformes du cadre juridique de l'Union européenne et de la convention 108, ainsi que sur les questions liées à la surveillance des autorités de la sécurité nationale. La Conférence a adopté deux résolutions:

- La première concerne le cadre de coopération des autorités de protection des données. Elle appelle les autorités de protection des données en Europe à mettre en place une coopération plus étroite, effective et proactive. Ces autorités doivent pouvoir agir en toute indépendance et bénéficier des ressources nécessaires à l'accomplissement de leurs tâches.
- Une seconde résolution concerne les flux transfrontières de données. Elle met en particulier l'accent sur la responsabilité des autorités de protection des données dans l'information des personnes concernées quant à leurs droits lors du transfert de données personnelles à l'étranger.

Conférence internationale des commissaires à la protection des données et à la vie privée

La 38^e conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue en 2016 à Marrakech. Elle a réuni quelque 500 participants provenant de 70 pays qui ont débattu des enjeux actuels de la vie privée et notamment de l'impact des technologies et de l'importance de l'éducation au numérique. Durant la conférence fermée, les commissaires ont abordé la question de l'intelligence artificielle et de la robotique, ainsi que celui de la cryptographie. À l'instar de toutes les nouvelles technologies de l'information et des communications, l'intelligence artificielle et la robotique suscitent de nouveaux défis pour le droit à la protection des données. L'intelligence artificielle et les robots permettent de simuler les caractéristiques humaines en offrant des fonctions d'aides aux utilisateurs ou en exécutant des tâches accomplies par l'homme. De plus en plus, ces machines vont prendre des formes humanoïdes et interagir avec les humains. Ces outils sont équipés de nombreux senseurs et sont connectés; ils sont en mesure de collecter des masses d'informations et de se remémorer tous les événements qui se sont produits dans leur environnement. Ils présentent néanmoins encore une part d'imprévisibilité dans les résultats issus du traitement de

données. Cela pose la question de la responsabilité lors de la prise de décision automatisée, notamment si les algorithmes utilisés parviennent à des conclusions inconnues pour le développeur ou l'utilisateur de l'application. Il y a également un risque de manipulation des individus pour orienter leur comportement ou leur décision. En soi, les robots n'ont pas de mémoire sélective et ils sont à même, selon la manière dont ils ont été programmés, de se souvenir de tout. La question se pose, si on devrait dès lors fixer des règles, notamment limitant la mémoire, garantissant la transparence des processus de traitement et offrant un contrôle sur celle-ci afin d'éviter des dérives. L'homme doit demeurer responsable des données enregistrées par le robot. Il y a un enjeu de société crucial, à savoir nous devons définir jusqu'où nous voulons et pouvons accepter que l'intelligence artificielle détermine nos choix et nos actions ?

La question du chiffrement ou du cryptage des données a également fait l'objet de débats au sein de la conférence. Cette technologie est un mécanisme important pour le monde du commerce et des affaires, ainsi que pour les consommateurs et les personnes concernées par le traitement de données personnelles. Le cryptage permet de sécuriser l'information notamment lors de transactions, de communication et de stockage des données. Il peut entraîner des difficultés pour les autorités de poursuite pénale, notamment lors de l'interception des communications. Face à des intérêts antagonistes, aucune réponse satisfaisante n'a encore été apportée. La majorité des experts ne sont pas favorables à l'introduction d'une vulnérabilité sélective des programmes de chiffrement car cela entraînerait un affaiblissement de la sécurité des données.

La Conférence a fait le point sur différentes initiatives en cours. Elle a ainsi pris connaissance du rapport intermédiaire du rapporteur spécial des Nations Unies pour le droit à la vie privée. Nous avons également informé la conférence des travaux du groupe de travail sur l'action humanitaire. La conférence a enfin adopté quatre résolutions, à savoir:

- une résolution pour l'adoption d'un référentiel international d'éducation des données personnelles. Cette résolution est accompagnée d'un premier référentiel de formation des élèves à la protection des données personnelles;
- une résolution sur le développement de nouveaux indicateurs de la protection des données afin d'avoir des informations comparables des différentes politiques de vie privée dans le monde;
- une résolution sur les défenseurs des droits de l'homme, dans laquelle les commissaires recon-

naissent le travail essentiel des défenseurs des droits de l'homme pour la création de société solide, durable et démocratique et leur rôle clé pour atteindre pleinement l'État de droit et renforcer la démocratie;

- une résolution sur la coopération internationale.

Association francophone des autorités de protection des données (AFAPDP)

L'AFAPDP s'est réunie en conférence en 2016 à Ouagadougou, au Burkina Faso. À cette occasion, les participants ont débattu de la sécurité des données, des analyses de risques de la protection des données, de la protection des données dans le domaine de la recherche et de l'accès aux bases de données des opérateurs de télécommunications par les services de sécurité. Cela a permis de nombreux échanges sur les législations et les différentes pratiques dans les États francophones. L'AFAPDP a adopté une résolution sur le droit à l'oubli par laquelle l'association attire l'attention sur les discussions qui ont eu lieu à l'échelle régionale et internationale sur l'application du droit à l'effacement et au déréférencement pour les moteurs de recherche et sur les mesures de protection de la réputation en ligne. Elle appelle les États et gouvernements de la Francophonie à reconnaître un droit à l'effacement et au déréférencement de portée universelle. L'AFAPDP a en outre procédé à l'élection de son bureau et porté à sa présidence le préposé fédéral suppléant.

1.10.2 Groupes de coordination de contrôle SIS II, VIS et Eurodac

En 2016, les groupes de coordination de contrôle des systèmes SIS II, VIS et Eurodac ont siégé deux fois.

Les groupes de coordination de contrôle du système d'information Schengen SIS II, du système d'information sur les visas (VIS) et d'Eurodac se sont réunis à Bruxelles en avril 2016 ainsi qu'en novembre 2016 (les trois groupes ont siégé à chaque fois successivement). Des informations concernant les trois groupes de coordination sont disponibles sur le site Internet du Contrôleur européen de la protection des données. On y trouve des comptes-rendus des réunions ainsi que les documents publiés, rapports d'activités, prises de position communes, etc.

1.10.3 Groupe de travail «Border, Travel & Law Enforcement»

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

Le sous-groupe a notamment traité de la question du bouclier de protection des données UE-États-Unis (Privacy Shield) qui permet à certaines conditions le transfert de données personnelles de l'UE à une société aux États-Unis (cf. aussi chiffre 1.8.1 du présent rapport). Il suit avec une attention particulière l'avancée du projet de «frontières intelligentes» suite à l'adoption par la Commission d'une proposition de règlement portant sur la création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne ainsi que les travaux du groupe d'experts mis en place dans ce contexte. Le groupe a d'ailleurs adressé une lettre au président de la commission des libertés civiles, de la justice et des affaires intérieures. Il a accompagné l'«accord parapluie» qui encadre les échanges de données personnelles en matière de police et de justice en limitant les droits des administrations américaines dans le traitement des données européennes, les travaux du Comité de la Convention sur la Cybercriminalité du Conseil de l'Europe ainsi que la création d'un cadre européen pour la communication des données PNR aux pays tiers et pour l'utilisation de ces à des fins répressives. Enfin, le sous-groupe de travail a commencé ses travaux en vue de la transposition de la Directive UE 2016/680.

1.10.4 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 coopérer avec les acteurs concernés, un groupe de travail piloté par notre autorité a été créé.

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. Le groupe de travail est piloté par un représentant de notre autorité. Le groupe de travail s'est fixé les objectifs principaux suivants: identifier 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.

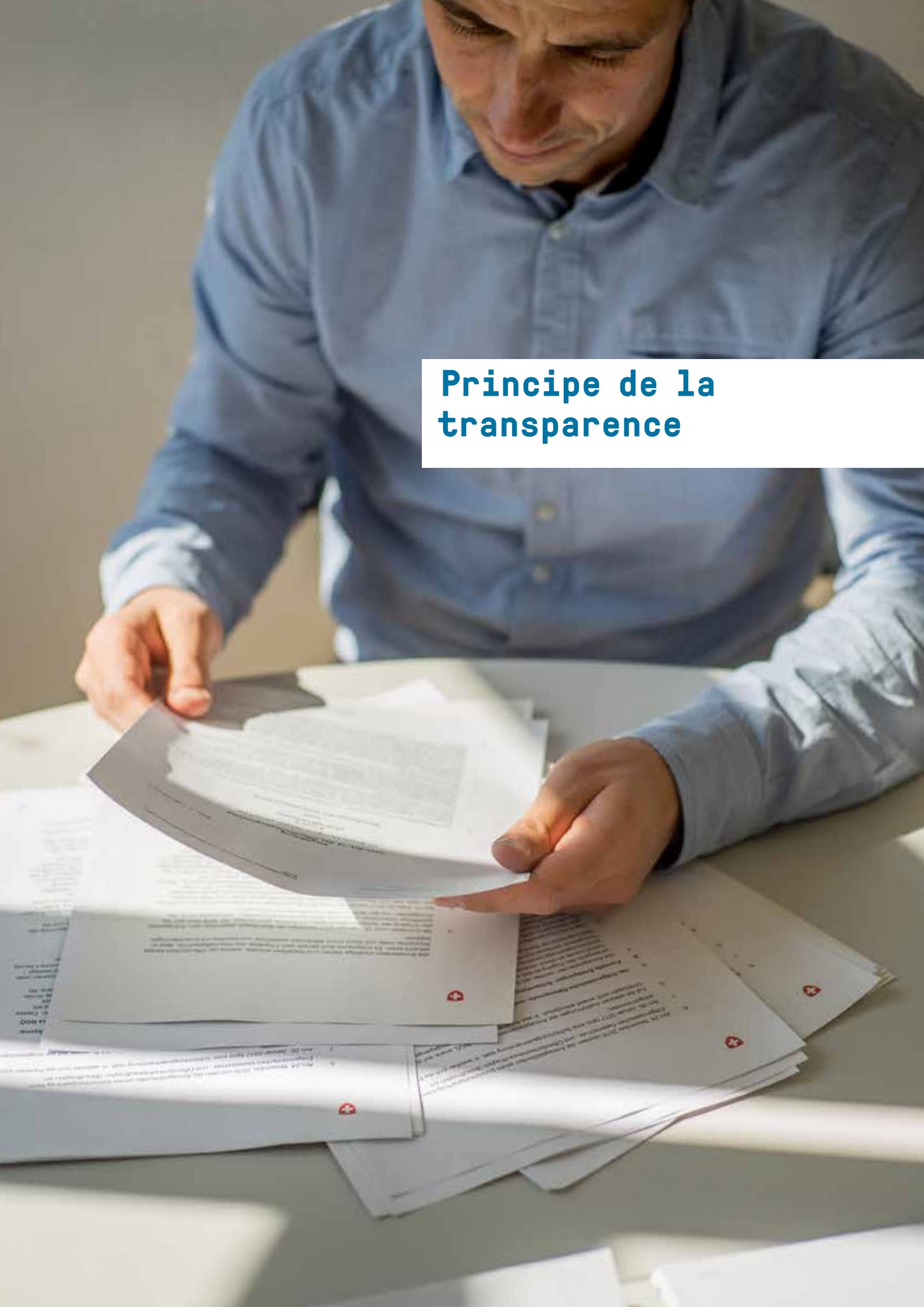
Tout au long de l'année 2016, le groupe a principalement poursuivi deux pistes de travail. Il a d'un part développé l'expertise des autorités de protection des données dans le domaine humanitaire à travers des recherches et des rencontres. D'autre part, il a travaillé avec les acteurs humanitaires internationaux, 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 est de faire le lien entre action humanitaire et 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.

Le BPH et le CICR sont à l'origine de cette initiative et ont associé le groupe de travail ainsi que deux autres membres de la CICPDVP: le Contrôleur européen de la protection des données et le Conseil de l'Europe. Le projet consiste en une série de six ateliers thématiques organisés tout au long de l'année 2016 et chaque atelier a donné lieu à la rédaction de recommandations par les participants. Un manuel compilant toutes ces recommandations est en cours d'élaboration. Il sera publié afin

de pouvoir proposer des lignes directrices protectrices des données personnelles à l'attention des acteurs humanitaires. Leur publication est prévue pour mi-2017.

Le groupe de travail va poursuivre ses activités avec le CICR et le BPH, notamment en continuant à s'impliquer dans la préparation de la version finale du manuel.

Principe de la transparence



2.1 Demandes d'accès

Selon les chiffres qui nous ont été communiqués pour l'année 2016, 551 demandes d'accès ont été soumises aux autorités fédérales (en incluant le Ministère public de la Confédération et les Services parlementaires, le nombre de demandes d'accès s'élève à 558, cf. 2.1.2 s.). Ce chiffre représente une diminution d'environ 50 demandes par rapport à l'année 2015. Dans 303 cas (55%) les autorités ont accordé un accès complet alors que dans 105 cas (19%), les demandeurs n'ont reçu qu'un accès partiel aux documents. Pour 87 cas (16%), l'accès a été entièrement refusé. Par ailleurs, les autorités ont annoncé que 26 demandes d'accès ont été retirées et que 33 demandes étaient encore en suspens à la fin de l'année 2016. 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.

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'OFEV qui a reçu le plus de demandes d'accès en 2016 (27), suivi du SEM (26) et de l'OFAG (23). Les départements ayant reçu le plus de demandes sont le DFAE (118), suivi du DETEC (89) et du DEFR (85). Les chiffres du DFAE témoignent d'une grande ouverture à la transparence avec 86 réponses positives sur 118 demandes; dans onze cas, l'accès a été partiellement accordé ou reporté et entièrement refusé dans 16 autres. Sur 71 autorités, 13 nous ont annoncé qu'aucune demande ne leur avait été soumise pendant l'année 2016. Lors de la même année, le Préposé a pour sa part reçu dix demandes. Il a entièrement accordé l'accès dans huit cas, il l'a partiellement accordé dans un autre cas et, dans le cas restant, les documents officiels n'existaient pas.

En 2016, le total des émoluments perçus pour l'accès à des documents s'élève à 22 770 francs. Il s'agit d'un montant largement plus élevé que celui perçu lors des années précédentes (2015: 13 663 fr.; 2014: 2600 fr.; 2013: 6502 fr.). Le Préposé remarque que l'augmen-

tation considérable des émoluments prélevés va dans le sens contraire de l'initiative parlementaire de la conseillère nationale Edith Graf-Litscher réclamant la gratuité pour des documents officiels. Ce montant de 22 770 francs a été prélevé pour 13 des 550 demandes d'accès déposées en 2016. Comme lors des années précédentes, le prélèvement d'un émolument a constitué l'exception; la gratuité ayant été accordée dans presque 98 pour cent des cas. Il convient 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 prélevé aucun émolument, les six autres départements ont partiellement facturé leur temps de travail aux demandeurs. La majeure partie des montants facturés l'ont été par le DEFR (12 730 fr. pour deux demandes), le DFJP (4000 fr. pour une demande) et le DDPS (2660 fr. pour deux demandes).

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 a de nouveau augmenté par rapport aux années précédentes (2016: 3301 heures; 2015: 2912 heures; 2014: 1707 heures). En revanche, le temps de travail investi dans la participation à des procédures de médiation a nettement diminué: il est passé de 1148 heures en 2015 à 857 heures en 2016. Le temps de travail consacré à l'établissement d'une décision ou à une éventuelle procédure de recours n'a pas été comptabilisé ou ne l'a pas été séparément.

2.1.2 Services parlementaires

Les Services parlementaires nous ont annoncé avoir reçu trois demandes d'accès en 2016. L'accès a été accordé dans deux cas et refusé dans le troisième.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a annoncé avoir reçu quatre demandes pour lesquelles l'accès a été accordé entièrement trois fois et une fois partiellement.

2.2 Demandes en médiation

En 2016, 149 demandes en médiation ont été déposées auprès du Préposé, ce qui correspond à une augmentation de 52 pour cent par rapport à 2015 (98). Contrairement à cette année, la plupart des demandes déposées en 2016 ne proviennent pas des médias (23) mais des particuliers (99).

Ces chiffres permettent le constat suivant: dans 192 cas, l'Administration fédérale a refusé l'accès de manière totale (87) ou partielle (105). Ces données sont à mettre en perspective avec les 149 demandes en médiation qui sont parvenues au Préposé. Pendant l'année sous revue, plus de 77 pour cent des cas de demandes d'accès totalement ou partiellement refusées (2015: 43%), ont fait l'objet d'une demande en médiation

Au total, 159 demandes en médiation ont été réglées en 2016, parmi lesquelles 119 ont été soumises au cours de cette même année, 36 en 2015, trois en 2014 et une en 2013. Dans 19 cas, une solution consensuelle entre les participants a été trouvée. Parmi ces cas, à onze reprises une médiation au sens propre a permis d'arriver à une solution et les huit cas restants ont été résolus à l'amiable grâce à l'intervention du Préposé. Dans cinq cas, l'accès a été accordé après l'ouverture de la procédure de médiation sans intervention du Préposé. Ce dernier a émis en tout 32 recommandations lorsqu'aucune solution amiable ne paraissait envisageable. Ces 32 recommandations ont permis de traiter 122 demandes en médiation. Cette différence s'explique principalement par le fait qu'une même recommandation a permis de clore 74 cas. Par ailleurs, quatre demandes en médiation ont été retirées. Dans cinq cas, les conditions d'application de la LTrans n'étaient pas remplies et dans quatre autres, la demande en médiation n'avait pas été soumise dans les délais. Enfin, deux procédures en médiation ont été suspendues.

Pendant l'année sous revue, le nombre de procédures de médiation menées à terme a sensiblement augmenté (+ 25 procédures), ce qui s'explique en premier lieu par la présence de deux collaborateurs supplémentaires dont les contrats de travail étaient de durée déterminée (mai-décembre 2016). Toutefois, le retard pris dans le traitement des procédures de médiation en suspens n'a pas pu être entièrement résorbé. Pour tenter de palier au nombre important de procédures pendantes, le Préposé va appliquer une nouvelle méthode de travail pendant l'année 2017 (cf. chiffre 2.4.1 du présent rapport).

Toutes les recommandations émises pendant l'année sous revue sont disponibles sur le site internet du Préposé (www.leprepose.ch, Principe de la transparence – Recommandations).

2.3 Consultations des offices

2.3.1 Restriction du principe de la transparence dans le domaine de la surveillance des transports publics

Le Conseil fédéral souhaite exclure de la loi sur la transparence les rapports d'audit et de contrôle de l'Office fédéral des transports (OFT) concernant la sécurité des chemins de fer et des bateaux. Cette décision ressort de l'approbation, lors de sa séance du 16 novembre 2016, du projet de loi concernant l'organisation de l'infrastructure ferroviaire (OBI). Le Préposé s'est opposé à cette restriction du principe de la transparence.

L'OFT avait prévu quatre dispositions spéciales identiques dans la loi fédérale sur les chemins de fer (LCdF), la loi fédérale sur les installations à câbles transportant des personnes (LICa), la loi fédérale sur le transport des voyageurs (LTV) et la loi fédérale sur la navigation intérieure (LNI). Conformément à ces dispositions, la LTrans ne s'appliquerait plus aux rapports concernant les audits, les contrôles d'exploitation et les inspections de l'OFT, ainsi qu'à tous les autres documents officiels concernant la sécurité technique ou la sécurité de l'exploitation s'ils contiennent des données personnelles. Selon l'OFT, il s'agirait là du seul moyen pour empêcher que les entreprises contrôlées retiennent des informations nécessaires à assurer la sécurité, et ce, en dépit de leurs obligations légales d'informer et de renseigner.

A notre avis, le régime d'exceptions prévues par la LTrans permet déjà de tenir suffisamment compte des intérêts à la confidentialité dans le cadre des mesures de contrôle effectuées par les autorités. La loi prévoit en particulier que l'administration peut fournir des garanties de confidentialité aux entreprises souhaitant divulguer des informations. L'État de droit implique que les obligations légales sont respectées et appliquées. Ce principe a également été confirmé par le Tribunal administratif fédéral dans son arrêt du 10 août 2016, entre-temps porté devant le Tribunal fédéral. Le tribunal y établissait en outre l'existence d'un intérêt public prépondérant dans la communication d'informations sur la mise en danger et la perturbation des transports publics. Si l'ensemble de l'activité de surveillance de l'OFT était ainsi soustrait à la LTrans, il pourrait en résulter un domaine (secret) de l'action de l'État entièrement soustrait au contrôle du public. Dans le cadre de la consultation des offices, nous avons donc rejeté les restrictions prévues.

Le 16 novembre 2016, le Conseil fédéral a proposé, malgré nos objections, l'introduction de ces restrictions controversées par la voie d'un projet spécial de politique des transports. A notre avis, il aurait été plus approprié de les traiter dans le cadre de la question, toujours en suspens, de la nécessité d'une révision de la LTrans.

2.3.2 Accès aux documents relatifs aux marchés publics

L'acquisition de biens et de services par l'administration fédérale revêt un intérêt public particulier. Nous avons donc pris position contre le projet de l'Office fédéral des constructions et de la logistique (OFCL) visant à exclure du champ d'application de la loi sur la transparence les documents concernant les acquisitions. Le droit d'accès accordé actuellement à la population et aux médias serait supprimé.

La loi fédérale sur les marchés publics (LMP) et l'ordonnance y relative font actuellement l'objet d'une révision totale. Bien que cela n'ait été prévu ni dans la procédure de consultation, ni dans la consultation des offices, le Conseil fédéral a récemment adopté un projet de loi prévoyant des règles spéciales vis-à-vis de la LTrans, qui figurent sous les titres «Conservation de documents» et «Droit de regards». Ainsi, selon l'article 49 LMP, tous les documents devront être tenus secrets pendant la durée de leur conservation, à moins que la présente loi ne prévoient leur publication. Seraient réservés les devoirs légaux d'information à l'égard des autorités pour autant qu'une base légale existe dans le droit fédéral ou le droit cantonal. Toujours selon le projet de loi (art. 59), tous les documents relatifs à la vérification du prix par le Contrôle fédéral des finances doivent rester secrets. Donc eux aussi, de l'avis du Conseil fédéral, seraient entièrement soustraits du champ d'application de la LTrans.

Nous nous sommes déjà exprimés, avant la décision du Conseil fédéral, contre les deux réglementations, d'autant que la publication des dépenses sur la plate-forme simap.ch n'offre pas d'accès public aux documents concernant les marchés publics: si cet accès aux marchés publics demeurerait exclu à l'avenir, l'objectif déclaré de transparence de la LMP révisée serait contourné, et la LTrans serait vidée de son sens. En particulier dans le domaine sensible des marchés publics, il est indispensable de garantir une application sans restriction de la LTrans. Grâce à cet accès de la population et des médias, de graves blocages de marchés publics, qui auraient pu coûter cher aux contribuables,

ont pu être révélés par le passé, et cela a permis de tirer les enseignements qui s'imposaient.

Lorsque les documents de marchés publics contiennent des secrets commerciaux, ceux-ci sont explicitement protégés par la LTrans. Rien ne justifie donc l'exclusion de ces documents ou d'autres documents officiels de son champ d'application (cf. également 22^e rapport d'activités 2014/2015, chiffre 2.2.3). La décision du Parlement sur cette question n'a pas encore été rendue.

2.3.3 Ordonnance sur le Service de renseignement

Le projet d'ordonnance relative à la nouvelle loi sur le Service de renseignement contient une disposition qui permettrait d'exclure de la loi sur la transparence pratiquement tous les documents émanant du Service de renseignement de la Confédération. Nous nous sommes opposés à cette réglementation.

La nouvelle loi sur le renseignement (LRens) qui entrera en vigueur le 1^{er} septembre 2017 soustraira de la LTrans l'accès aux documents officiels portant sur la recherche d'informations. Le projet de la disposition d'exécution destinée à figurer dans l'ordonnance sur le Service de renseignement (ORens) prévoit pour sa part que cette exception à la LTrans devait valoir pour tous les documents officiels permettant de tirer des conclusions directes ou indirectes sur la recherche d'informations conformément au chapitre 3 LRens. Cette disposition cite ensuite trois exemples de cas d'application: les informations entrantes ou se fondant sur des produits classifiés du renseignement, les informations sur les moyens, méthodes et contacts en matière de renseignement du SRC ou des services qu'il a mandatés, ainsi que les informations sur les appareils, systèmes et infrastructures mis en œuvre.

Au cours de la procédure de consultation, nous avons rejeté ce projet de disposition d'exécution et fait observer que cette formulation permettrait d'exclure de la LTrans presque toutes les informations que le SRC reçoit ou génère. Cela reviendrait à exclure totalement le SRC, ce qui n'est toutefois pas l'intention du législateur. Nous renvoyons à cet égard à la disposition de la loi sur le Service de renseignement qui limite sans équivoque à la recherche d'informations la norme spéciale relative à la LTrans. En vertu d'un raisonnement a contrario, toutes les autres tâches du SRC qui ne se rapportent pas en tant que telles à la collecte d'informations, comme

les estimations de situation, les analyses et les évaluations, devraient continuer à être régies par la LTrans et ses dispositions d'exécution.

Nous avons insisté sur le fait que, conformément au principe de légalité, les prescriptions détaillées d'une ordonnance ne peuvent que préciser une réglementation déjà présente dans la loi. Or la disposition prévue dans le projet d'ordonnance élargissait l'exception figurant dans la loi de manière abusive à presque tous les documents du SRC.

Enfin, nous avons expressément souligné que les informations ne concernant pas la recherche d'informations ne seraient pas accessibles au public dans tous les cas. En fait, les exceptions prévues dans la LTrans pourraient s'appliquer au cas par cas.

Nos propositions visant à faire adapter cette disposition n'ont pas été prises en compte. Le projet d'ordonnance est encore en consultation.

2.4 Varia

2.4.1 Nouvelle méthode de travail concernant la tenue des procédures de médiation

Depuis le 1^{er} janvier 2017, les nouvelles demandes de médiation sont en majorité traitées dans le cadre de procédures orales et accélérées. Cette méthode a pour but de diminuer la durée de traitement des procédures de médiation.

Le principe de célérité est un principe fort de la LTrans; il s'exprime dans les délais d'ordre des différentes étapes de la procédure (appréciation de la demande déposée par les autorités, procédure de médiation, procédure de décision). Le Préposé entend désormais traiter les demandes de médiation dans le délai légal de 30 jours. Pour ce faire, il faut accélérer les procédures de médiation. De l'avis du Préposé, le meilleur moyen d'atteindre cet objectif est de traiter en majorité oralement les demandes de médiation, et non plus par écrit comme c'était le cas jusqu'ici.

Dans le cadre d'un essai d'un an à partir du 1^{er} janvier 2017, les nouvelles demandes et, dans la limite du raisonnable, les demandes de médiation déjà en cours de traitement sont donc traitées majoritairement au moyen de médiations orales en présence des personnes et des offices concernés. De ce recours plus fréquent à la médiation orale, le Préposé n'attend pas seulement une réduction de la durée des procédures de médiation, mais aussi une augmentation du nombre des solutions consensuelles. Dans certains cas précis (par ex. problématiques juridiques nouvelles ou difficiles, situations d'accès complexes), le Préposé se réserve toutefois de recourir aux procédures écrites comme c'était le cas auparavant.

Etant donné le grand nombre de recommandations et d'arrêts du Tribunal fédéral rendus depuis l'entrée en vigueur de la LTrans, le Préposé est convaincu que cette nouvelle méthode accélèrera les procédures de médiation et permettra de réduire le nombre des décisions des autorités. Les premières expériences sont positives.

2.4.2 Les dix ans de la loi sur la transparence

A l'occasion des dix ans de la LTrans, le Préposé a organisé le 2 septembre 2016 avec l'Office fédéral de la justice la deuxième Journée suisse du principe de la transparence dans l'administration publique. Cette manifestation a rassemblé principalement des représentants de l'administration fédérale et des cantons ainsi que des journalistes. Les conférenciers se sont penchés sur le thème de la rencontre «10 ans de loi sur la transparence: notre administration fédérale est-elle devenue plus transparente?» en se plaçant sous différents points de vue. Le Préposé a présenté à cette occasion la nouvelle procédure accélérée appliquée depuis janvier 2017 (cf. chiffre 2.4.1 du présent rapport). Les présentations des conférenciers peuvent être consultées sur le site du Préposé www.leprepose.ch à la rubrique Actualités – Manifestations – 2016-2017.



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 transparence (LPD) a fluctué entre 20 et 24. Les 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 la promulgation de lois spéciales dans le secteur de la santé n'ont pas pu être tous pourvus en raison de mesures d'économie.

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

Prestations

Selon le Nouveau modèle de gestion pour 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 | 18.2 % | |
| Conseil Confédération | 15.7 % | |
| Collaboration avec les cantons | 4.0 % | |
| Collaboration internationale | 11.1 % | |
| Total Conseils | | 49.0 % |
| Surveillance | 14.6 % | |
| Certification | 0.1 % | |
| Registre des données | 0.9 % | |
| Total Surveillance | | 15.6 % |
| Information | 12.2 % | |
| Formation/Conférences | 5.9 % | |
| Total Information | | 18.1 % |
| Législation | 17.3 % | |
| Total Législation | | 17.3 % |
| Total Protection des données | | 100.0 % |

Conseil

Comme nous l'avons exposé au chapitre «Défis actuels et priorités», le PFPDT est confronté à une demande croissante dans le domaine du conseil, en raison de l'extension de son domaine de compétence et des besoins grandissants en accompagnement de projets. En 2016, environ 50 pour cent des ressources ont été affectées aux prestations de conseil. Selon la planification du PFPDT pour l'année 2017, l'accompagnement de dix grands projets est en cours.

| Conseil grands projets 2017 | |
|---|---|
| Transport | 3 |
| Finances | 1 |
| Santé et travail | 3 |
| Sécurité | 1 |
| Télécommunication / Internet des objets | 2 |

Comme les ressources du PFPDT n'ont à ce jour pas été adaptées à l'augmentation des risques d'identification rétroactive, ni aux autres défis de la numérisation, il n'est 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.

Surveillance

Comme nous l'avons exposé plus haut, 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 inférieur à la moyenne à long terme de 20 pour cent. Selon la planification pour l'année 2017, ces ressources devront venir à bout de huit contrôles de grande envergure. Si l'on compare ce nombre aux 12 000 grandes et moyennes entreprises que compte la Suisse, la densité de contrôle actuelle apparaît faible.

Législation

L'évolution technologique, que le Conseil fédéral a qualifiée de «fulgurante», se répercute aussi sur le traitement des données par les organes fédéraux. Elle se traduit par de très nombreuses prescriptions de traitement dans la législation spéciale de la Confédération, 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, et la tendance se poursuit.

Révision totale de la LPD

Pour la mise en œuvre des objectifs réglementaires mentionnés, qui est également l'objet de l'avant-projet de révision totale de la loi fédérale sur la protection des données (AP-LPD), de nouveaux instruments sont prévus, comme par exemple les recommandations de bonnes pratiques ou les analyses d'impact relatives à la protection des données, qui doivent être repris des règlements du Conseil de l'Europe et de l'UE. La mise en œuvre de ces instruments repose le plus souvent sur une interaction entre les responsables d'applications et l'autorité de protection des données.

Selon le rapport explicatif concernant l'AP-LPD, le Conseil fédéral estime que le besoin en ressources du PFPDT devrait «augmenter significativement». De la

quantification effective de ce renforcement des ressources dépendra l'intensité avec laquelle l'autorité de protection des données de la Confédération pourra mener à bien sa mission. Comme les nouveaux instruments sont décrits de manière générale dans le texte de loi, il apparaît clairement que les autorités politiques disposent d'une marge de manœuvre considérable pour apprécier les évolutions futures et les quantifier.

Les organes politiques doivent à cet égard porter l'attention requise à la mission du PFPDT: la tâche principale de l'autorité de protection des données 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. |
| 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 1^{er} janvier 2017 une procédure sommaire et accélérée, caractérisée par la généralisation des médiations orales.

L'expérience des premiers mois est positive: la durée de traitement des nouvelles demandes en médiation a pu être considérablement réduite, et on observe

une hausse de la proportion de solutions amiables entre les requérants et les autorités. De plus, le PFPDT est parvenu à réduire ses coûts en remettant non plus des recommandations détaillées, mais des recommandations sommaires. Cela a toutefois impliqué un temps de travail accru pour le Préposé et pour le responsable du domaine de direction LTrans, qui mènent toujours personnellement les négociations de médiation et assistent parfois à quatre séances par semaine. Au premier semestre 2018, un rapport d'évaluation permettra de savoir si les retards accumulés peuvent être résorbés avec les effectifs actuels.

3.2 11^e journée de la protection des données – Les limites de la vidéosurveillance

La journée de la protection des données 2017 a été l'occasion pour nous de nous exprimer au sujet des risques relatifs à la vidéosurveillance. Les particuliers sont eux aussi de plus en plus nombreux à utiliser des installations de vidéosurveillance pour sécuriser leur propriété ou leur entreprise. Une utilisation conforme à la protection des données requiert le respect de certains principes.

Comme le prix des caméras vidéo ne cesse de baisser, leur emploi pour la surveillance dans le domaine privé se popularise. De même, les particuliers les fixent sur des drones ou les utilisent comme caméras embarquées dans des véhicules (dashcams). Toutes ces utilisations peuvent impliquer des intrusions dans la sphère privée de tiers. La vidéosurveillance est devenue une thématique multi-forme, qui concerne et intéresse de larges catégories de la population, avec des répercussions sur notre activité consultative. Dans les médias également, la vidéosurveillance est un thème récurrent.

Depuis 2007, la journée mondiale de la protection des données est organisée chaque année le 28 janvier, à l'initiative du Conseil de l'Europe, dans toute l'Europe et au-delà. Son objectif est de sensibiliser les citoyens aux thèmes de la protection de la sphère privée et du droit à l'autodétermination informationnelle, pour initier un changement durable des comportements à l'égard des nouvelles technologies.

Nous avons publié sur notre site Internet une nouvelle page intitulée «Vidéosurveillance effectuée par des particuliers», offrant un aperçu des différentes formes de la vidéosurveillance et des risques qui y sont associés, et informant à la fois les exploitants d'installations de vidéosurveillance sur leurs obligations et les personnes affectées sur leurs droits.

3.3 Publications et participation à des manifestations au cours de l'année sous revue

Notre site Internet www.leprepose.ch contient de nombreuses informations complètes sur les différents domaines d'activités du PFPDT. Durant l'année sous revue, nous avons notamment publié des explications concernant l'utilisation de capteurs fitness en lien avec les assurances ainsi que sur les aspects relatifs à la protection des données du protocole Internet IPv6. Nous avons par ailleurs participé à de nombreuses manifestations.

Mesurer ses propres paramètres corporels et performances au moyen d'applications de fitness ou de capteurs d'activités peut être motivant et s'avérer bénéfique pour la santé et le bien-être général. Ce faisant, les utilisateurs produisent une quantité considérable de données numériques, qui deviennent rapidement difficiles à gérer. Le risque d'une perte de contrôle est bien réel et menace le droit fondamental à l'autodétermination informationnelle (www.leprepose.ch, Protection des données – Santé – Assurance-maladie/accidents).

Internet est aujourd'hui la principale technologie pour tout type de communication. Comme les adresses IP du protocole Internet version 4 (IPv4) actuellement utilisé seront bientôt épuisées, un nouveau protocole (IPv6) a été développé. Par rapport à l'IPv4, le protocole IPv6 offre un certain nombre d'avantages pratiques, mais comporte également certains risques pour la protection des données et la sphère privée. Ces risques peuvent être minimisés grâce à des mesures techniques et organisationnelles adaptées (www.leprepose.ch, Protection des données – Internet et ordinateur).

Nous avons en outre remanié nos explications relatives à la vidéosurveillance sur le lieu de travail (www.leprepose.ch, Protection des données – Secteur du travail – Surveillance sur le lieu de travail). La vidéosurveillance est souvent utilisée dans des commerces, des établissements de restauration ou de loisirs, généralement dans le but de se protéger contre le vol ou de prévenir les actes de vandalisme contre le mobilier ou les installations sanitaires. Toutefois, on oublie souvent que les clients ne sont pas les seuls concernés: le personnel est lui aussi filmé, ce qui peut également poser problème en matière de protection des données.

Le 11 janvier 2017, le Conseil fédéral a pris bonne note de la mise en place d'un nouveau cadre pour la transmission des données personnelles de la Suisse vers les États-Unis. Ce cadre juridique, baptisé «Privacy Shield», remplace l'accord «Safe Harbor», jugé insuffi-

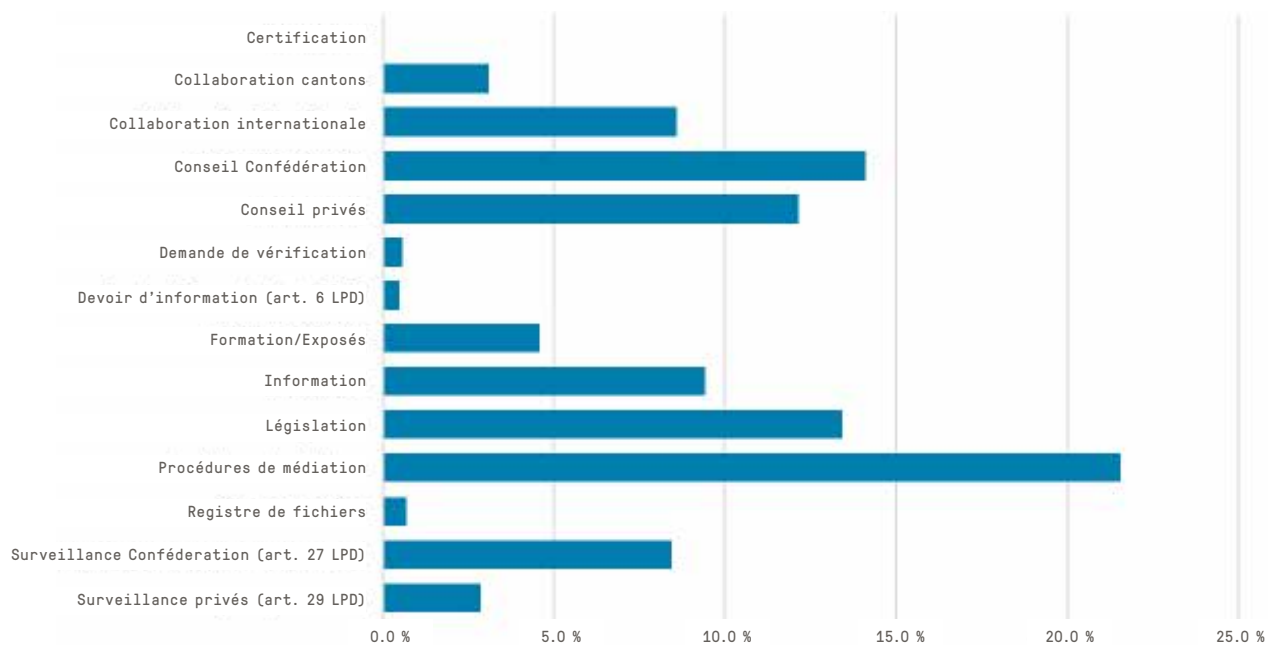
sant par le PFPDT et officiellement abrogé par le Conseil fédéral. Nous avons mis en ligne des informations complémentaires sur le Privacy Shield ainsi que les documents de référence (www.leprepose.ch, Protection des données – Commerce et économie – Transmission à l'étranger – États-Unis).

Durant l'année sous revue, de nombreuses entreprises, associations, organisations non gouvernementales et institutions ont demandé au Préposé de participer à leurs événements. En raison du manque de ressources, il n'a pas pu accepter toutes ces invitations. Il a tout de même participé à 80 podiums et conférences, sur diverses thématiques telles que transports, mégadonnées (big data), santé, société numérique ainsi que sur la révision de la LPD. En outre, il a entretenu des contacts réguliers avec les principaux acteurs économiques et politiques.

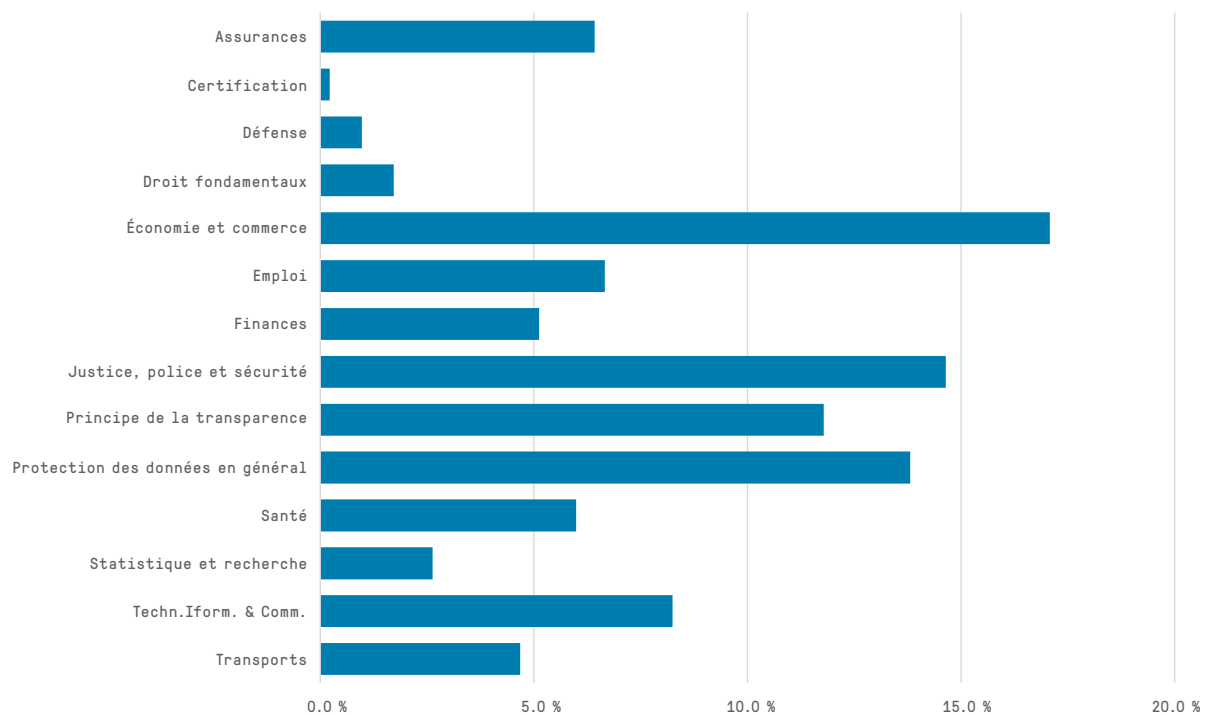
3.4 Statistiques

3.4.1 Statistiques des activités du PFPDT du 1^{er} avril 2016 au 31 mars 2016 (Protection des données et Principe de la transparence)

Charge de travail par tâches



Charge de travail par domaines



3.4.2 Statistique des demandes d'accès selon la loi sur la transparence du 1^{er} janvier 2016 au 31 décembre 2016

Chancellerie fédérale ChF

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| ChF | 19 | 9 | 2 | 3 | 4 | 1 |
| PPPDT | 10 | 8 | 0 | 1 | 0 | 0 |
| TOTAL | 29 | 17 | 2 | 4 | 4 | 1 |

Département fédéral des affaires étrangères DFAE

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| DFAE | 118 | 86 | 16 | 11 | 2 | 3 |
| TOTAL | 118 | 86 | 16 | 11 | 2 | 3 |

Département fédéral de l'intérieur DFI

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 6 | 2 | 2 | 2 | 0 | 0 |
| BFEG | 2 | 1 | 0 | 1 | 0 | 0 |
| OFC | 1 | 1 | 0 | 0 | 0 | 0 |
| AFS | 3 | 3 | 0 | 0 | 0 | 0 |
| MétéoSuisse | 0 | 0 | 0 | 0 | 0 | 0 |
| BN | 0 | 0 | 0 | 0 | 0 | 0 |
| OFSP | 16 | 7 | 2 | 3 | 3 | 1 |
| OFS | 6 | 2 | 2 | 1 | 1 | 0 |
| OFAS | 11 | 6 | 0 | 3 | 2 | 0 |
| OSAV | 7 | 2 | 0 | 3 | 0 | 2 |
| MNS | 0 | 0 | 0 | 0 | 0 | 0 |
| SWISSMEDIC | 19 | 7 | 6 | 5 | 0 | 1 |
| SUVA | 1 | 1 | 0 | 0 | 0 | 0 |
| TOTAL | 71 | 31 | 12 | 18 | 6 | 4 |

Département fédéral des finances DFF

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 8 | 2 | 3 | 3 | 0 | 0 |
| UPIC | 2 | 0 | 0 | 1 | 1 | 0 |
| AFF | 4 | 1 | 0 | 3 | 0 | 0 |
| OFPER | 3 | 2 | 1 | 0 | 0 | 0 |
| AFC | 5 | 2 | 1 | 2 | 0 | 0 |
| AFD | 13 | 3 | 7 | 1 | 1 | 0 |
| RFA | 3 | 2 | 1 | 0 | 0 | 0 |
| OFCL | 4 | 2 | 0 | 0 | 1 | 1 |
| OFIT | 3 | 3 | 0 | 0 | 0 | 0 |
| CDF | 6 | 4 | 1 | 1 | 0 | 0 |
| SFI | 3 | 1 | 2 | 0 | 0 | 0 |
| PUBLICA | 0 | 0 | 0 | 0 | 0 | 0 |
| CdC | 1 | 0 | 0 | 1 | 0 | 0 |
| TOTAL | 55 | 22 | 16 | 12 | 3 | 1 |

Département fédéral de justice et police DFJP

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 4 | 3 | 1 | 0 | 0 | 0 |
| OFJ | 1 | 1 | 0 | 0 | 0 | 0 |
| FEDPOL | 16 | 4 | 4 | 4 | 3 | 1 |
| METAS | 4 | 4 | 0 | 0 | 0 | 0 |
| SEM | 26 | 16 | 3 | 5 | 0 | 2 |
| ISDC | 6 | 5 | 0 | 1 | 0 | 0 |
| IPI | 1 | 1 | 0 | 0 | 0 | 0 |
| CFMJ | 0 | 0 | 0 | 0 | 0 | 0 |
| CAF | 0 | 0 | 0 | 0 | 0 | 0 |
| ASR | 0 | 0 | 0 | 0 | 0 | 0 |
| CSI | 0 | 0 | 0 | 0 | 0 | 0 |
| CNPT | 0 | 0 | 0 | 0 | 0 | 0 |
| TOTAL | 58 | 34 | 8 | 10 | 3 | 3 |

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 | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 7 | 5 | 0 | 0 | 1 | 0 |
| OFT | 7 | 5 | 1 | 0 | 1 | 0 |
| OFAC | 10 | 6 | 2 | 2 | 0 | 0 |
| OFEN | 12 | 8 | 0 | 3 | 1 | 0 |
| OFROU | 8 | 8 | 0 | 0 | 0 | 0 |
| OFCOM | 3 | 1 | 1 | 1 | 0 | 0 |
| OFEV | 27 | 18 | 3 | 3 | 0 | 3 |
| ARE | 0 | 0 | 0 | 0 | 0 | 0 |
| ComCom | 0 | 0 | 0 | 0 | 0 | 0 |
| IFSN | 11 | 1 | 1 | 4 | 4 | 1 |
| PostCom | 1 | 1 | 0 | 0 | 0 | 0 |
| AIEP | 3 | 3 | 0 | 0 | 0 | 0 |
| TOTAL | 89 | 56 | 8 | 13 | 7 | 4 |

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 | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 11 | 7 | 1 | 2 | 0 | 1 |
| Défense/armée | 5 | 1 | 2 | 2 | 0 | 0 |
| SRC | 8 | 0 | 1 | 1 | 3 | 3 |
| armasuisse | 17 | 0 | 5 | 3 | 2 | 7 |
| OFSPD | 2 | 1 | 1 | 0 | 0 | 0 |
| OFPP | 2 | 0 | 0 | 1 | 0 | 1 |
| TOTAL | 45 | 9 | 10 | 9 | 5 | 12 |

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 | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SG | 8 | 5 | 0 | 2 | 1 | 0 |
| SECO | 19 | 8 | 4 | 7 | 0 | 0 |
| SEFRI | 6 | 2 | 4 | 0 | 0 | 0 |
| OFAG | 23 | 4 | 5 | 12 | 2 | 0 |
| OFAE | 0 | 0 | 0 | 0 | 0 | 0 |
| OFL | 1 | 0 | 0 | 0 | 0 | 0 |
| SPr | 5 | 2 | 0 | 3 | 0 | 0 |
| COMCO | 16 | 13 | 1 | 1 | 0 | 1 |
| ZIVI | 1 | 0 | 0 | 1 | 0 | 0 |
| BFC | 1 | 1 | 0 | 0 | 0 | 0 |
| FNS | 0 | 0 | 0 | 0 | 0 | 0 |
| IFFP | 0 | 0 | 0 | 0 | 0 | 0 |
| Conseil des EPF | 5 | 2 | 1 | 2 | 0 | 0 |
| TOTAL | 85 | 37 | 15 | 28 | 3 | 1 |

Ministère public de la Confédération MPC

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| MPC | 4 | 4 | 0 | 0 | 0 | 0 |
| TOTAL | 4 | 4 | 0 | 0 | 0 | 0 |

Services du Parlement SP

| Section concernée | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|-------------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| SP | 3 | 2 | 1 | 0 | 0 | 0 |
| TOTAL | 3 | 2 | 1 | 0 | 0 | 0 |

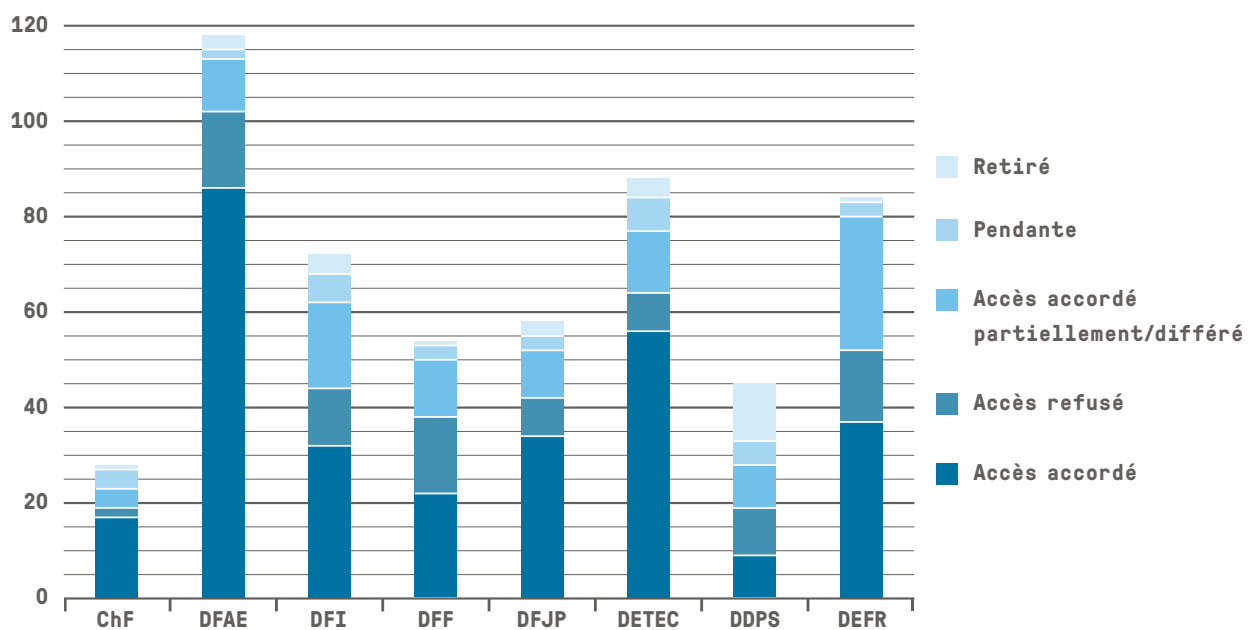
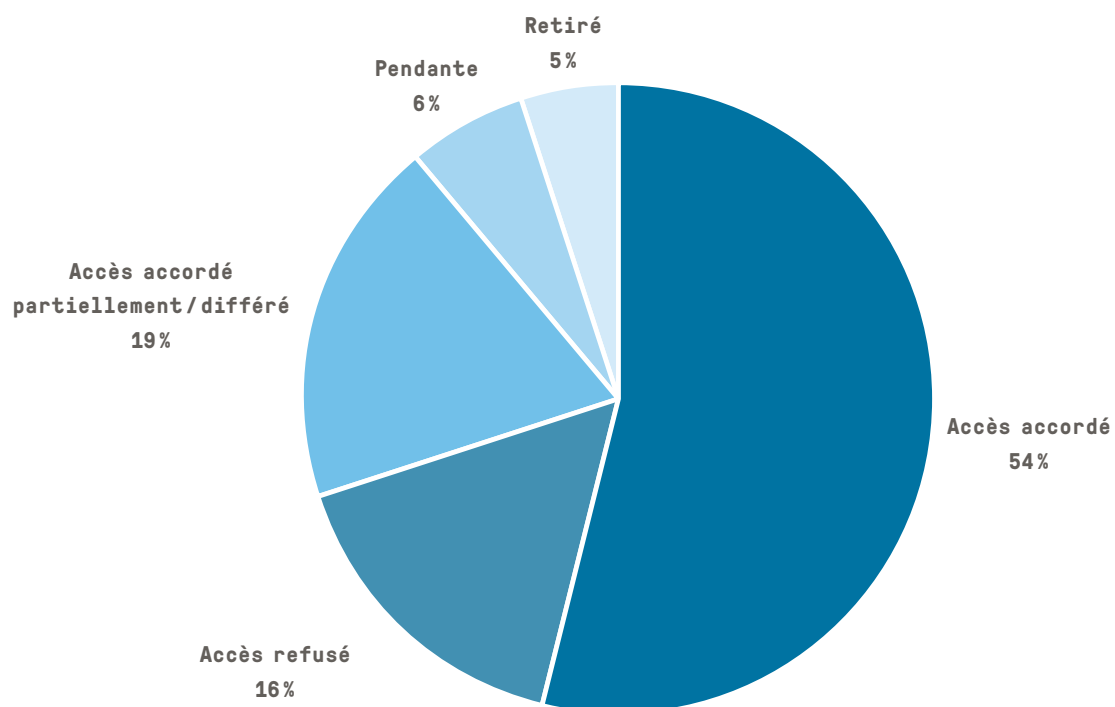
Vue d'ensemble des demandes d'accès de tous les départements et de la Chancellerie fédérale

| Département | Nombre de demandes d'accès | Accès accordé | Accès refusé | Accès accordé partiellement / différé | Demande d'accès pendante | Demande d'accès retiré |
|----------------|----------------------------|---------------|--------------|---------------------------------------|--------------------------|------------------------|
| ChF | 29 | 17 | 2 | 4 | 4 | 1 |
| DFAE | 118 | 86 | 16 | 11 | 2 | 3 |
| DFI | 72 | 32 | 12 | 18 | 6 | 4 |
| DFF | 55 | 22 | 16 | 12 | 3 | 1 |
| DFJP | 58 | 34 | 8 | 10 | 3 | 3 |
| DETEC | 89 | 56 | 8 | 13 | 7 | 4 |
| DDPS | 45 | 9 | 10 | 9 | 5 | 12 |
| DEFR | 85 | 37 | 15 | 28 | 3 | 1 |
| 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 | 2016 |
|--|------------|
| Médias | 23 |
| Personnes privées (ou requérants ne pouvant pas être attribués de manière précise) | 99 |
| Représentants de milieux intéressés (associations, organisations, sociétés, etc.) | 5 |
| Avocats | 2 |
| Entreprises | 20 |
| Total | 149 |

Traitement des demandes d'accès



3.5 Le Secrétariat du PFPDT

Préposé fédéral à la protection des données et à la transparence

Lobsiger Adrian (à partir du 1^{er} juin)

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

Team 2

Cheffe: Gloor Scheidegger Caroline, juriste

Koç Karin, juriste

Schönbett Frédéric, juriste

Trolliet Sabine, juriste

Team 3

Cheffe: Haag Sophie, juriste

Gisin Philipp, juriste

Rossier Odile, juriste

Domaine de direction Principe de la transparence

Chef: Ammann Reto

Team

Keller Annina, juriste

Moinat Marc, 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

Fuhrer Muriel, spécialiste technique I des services administratifs et commerciaux

Secteur Communication

Meier Francis, délégué d'information

Böhlen Silvia, spécialiste en communication

Secteur Société numérique

Responsable: Sidler Andreas

Fasel Frédéric, spécialiste technique I des services administratifs et commerciaux

Centre de compétence informatique

Cheffe: Gaukel Rahel, informaticienne

Aad Imad, informaticien

Scherrer Urs, informaticien

Stüssi Philipp, informaticien

Domaine de direction Relations internationales, Législation, Cantons

Chef: Walter Jean-Philippe

Team

Lenman Catherine, juriste

Liste des abréviations

| | |
|----------|---|
| AFC | Administration fédérale des contributions |
| AI | Assurance-invalidité |
| AVS | Assurance-vieillesse et survivants |
| BPH | Brussels Privacy Hub |
| CFF | Chemins de fer fédéraux |
| CICPDVP | Conférence internationale des commissaires à la protection des données et à la vie privée |
| CICR | Comité international de la Croix Rouge |
| COMAI | Centre d'observation médical de l'AI |
| CP | Code pénal suisse |
| DéICdG | Délégation des Commissions de gestion |
| DFJP | Département fédéral de justice et police |
| EAR | Echange automatique de renseignements |
| LA AF | loi sur l'assistance administrative fiscale |
| LAI | Loi fédérale sur l'assurance-invalidité |
| LEAR | Loi fédérale sur l'échange international automatique de renseignements en matière fiscale |
| LHR | Loi sur l'harmonisation des registres |
| LMSI | Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure |
| LOGA | Loi sur l'organisation du gouvernement et de l'administration |
| Loi e-ID | Loi fédérale sur les moyens d'identification électronique reconnus par l'État |
| LRens | Loi fédérale sur le renseignement |
| OAAF | l'ordonnance sur l'assistance administrative fiscale |
| OAMal | Ordonnance sur l'assurance-maladie |
| OCDE | Organisation de Coopération et de Développement Économiques |
| OEAR | Ordonnance sur l'échange international automatique de renseignements en matière fiscale |
| OFCL | Office fédéral des constructions et de la logistique |
| OFPER | Office fédéral du personnel |
| OFS | Office fédéral de la statistique |
| OFS | Office fédéral de la statistique |
| OFSP | Office fédéral de la santé publique |
| ORens | Ordonnance sur le renseignement |
| RAI | Règlement sur l'assurance-invalidité |
| SAS | Service d'accréditation suisse |
| SIS | Système d'information Schengen |
| SIS II | Système d'information de Schengen de deuxième génération |
| SMR | Service médical régional |
| SNA | Service national d'adresses |
| SRC | Service de renseignement de la Confédération |
| UTP | Union des transports publics |
| VIS | Système d'information sur les visas |

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, Peter Mosimann (Avant-propos)