22e Rapport d'activités 2014/2015

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2014/2015 du Préposé fédéral à la protection des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence est tenu de fournir périodiquement à l'Assemblée fédérale un rapport sur son activité (art. 30 LPD). Le présent rapport couvre la période du 1er avril 2014 au 31 mars 2015.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.022.d/f

Table des matières

Avant-propos 7

Liste des abréviations 11

1. Protection des données 14

1.1 Droits fondamentaux 14

1.1.1 Nouvelles directives sur la certification 14

1.1.2 Modifications du code civil – Infostar et registre foncier 15

1.1.3 Révision de la loi sur le registre du commerce 15

1.1.4 Projet de loi fédérale relative à l'application des principes du débiteur et de l'agent payeur à l'impôt anticipé 16

1.1.5 Projet MARS de l'Office fédéral de la statistique et de l'Office fédéral de la santé publique 17

1.1.6 Échange de données personnelles entre les registres des habitants, la Poste et d'autres détenteurs de données 18

1.1.7 Utilisation d'un identificateur universel de personnes dans la cyberadministration 20

1.2 Protection des données – Questions d'ordre général 22

1.2.1 Révision totale des systèmes d'information de la Confédération dans le domaine du sport 22

1.2.2 Système d'information concernant les voyageurs sans titre de transport valable 23

1.2.3 Stockage centralisé des photos de clients dans les stations de ski – explications générales 24

1.2.4 Surveillance vidéo dans les véhicules 24

1.2.5 Nouvelle loi sur les jeux d'argent 25

1.3 Internet et télécommunication 26

1.3.1 Externalisation dans le nuage du traitement des données par les organes fédéraux 26

1.3.2 Révision partielle de la loi fédérale sur la radio et la télévision – utilisation des numéros AVS par Billag 27

1.3.3 Nouveau service de bureautique au sein de l'administration fédérale (UCC) 28

1.3.4 Accès gratuit au réseau WiFi des CFF 29

1.3.5 Stratégie Open Government Data de la Confédération 30

1.3.6 Protection du droit d'auteur sur Internet 31

1.3.7 Publication sur Internet de rapports sur des enseignants 31

1.4 Justice/Police/Sécurité ... 33
1.4.1 Protection des données dans le cadre de la deuxième évaluation Schengen ... 33
1.4.2 Projet de loi sur le renseignement ... 34
1.4.3 Révision de l'ordonnance sur les systèmes d'information du SRC ... 35
1.4.4 Révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication ... 36
1.4.5 Révision de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (JANUS) ... 36
1.4.6 Modification des bases légales liées au développement de l'armée ... 37
1.4.7 Contrôle des logfiles auprès du Secrétariat d'État aux migrations en tant qu'utilisateur final du SIS ... 39
1.5 Santé et recherche ... 40
1.5.1 Remise du dossier médical original ... 40
1.5.2 Vente forcée de données de patients dans le cadre d'une procédure de faillite ... 41
1.5.3 Vol de données de patients dans un cabinet médical ... 41
1.5.4 Établissement des faits auprès du service médical de la Confédération (MedicalService AeD) ... 42
1.5.5 Conservation de dossiers médicaux dans le nuage ... 43
1.5.6 Cybersanté – Identification des patients et accès aux dossiers électroniques ... 44
1.5.7 Projet de loi fédérale sur l'enregistrement des maladies oncologiques ... 45
1.6 Assurances ... 47
1.6.1 Contrôle des services de réception des données auprès des assureurs-maladie ... 47
1.6.2 Format d'échange de données XML 4.4 pour les factures DRG ... 50
1.6.3 Assurances-maladies complémentaires: effacement des données figurant dans les demandes d'adhésion ... 51
1.6.4 Les procurations dans le domaine des assurances ... 52
1.6.5 Communication des données de l'assurance-maladie dans le cadre de la réduction des primes ... 53
1.7 Secteur du travail ... 54
1.7.1 Vidéosurveillance dans des établissements de restauration ... 54
1.7.2 Questionnaire de santé lors d'une candidature ... 54
1.7.3 Arrêt du Tribunal administratif fédéral concernant le bureau de communication pour lanceurs d'alerte (Whistleblowing) ... 55
1.7.4 Communication de renseignements dans le cadre d'une postulation ... 57

1.7.5 Transmission de données dans le domaine des mesures d'accompagnement ... 58
1.8 Économie et commerce ... 60
1.8.1 Smart grids et protection des données ... 60
1.8.2 Cartes clients dans le commerce de détail ... 60
1.8.3 Recherches dans le domaine des agences de renseignement économique et de renseignement en matière de crédit ... 61
1.8.4 Mise en œuvre du droit d'accès et du droit d'opposition par des maîtres de fichier ... 62
1.8.5 Communication de données de membres à des assurances ... 62
1.9 Finances ... 64
1.9.1 Clarifications relatives au traitement de données client chez Postfinance 64
1.9.2 Consultation en vue de l'échange automatique de renseignements fiscaux ... 65
1.9.3 Clôture de l'établissement des faits relatif au système de gestion des risques d'un institut financier ... 66
1.9.4 Externalisation à l'étranger de données bancaires pseudonymisées ... 67
1.10 International ... 70
1.10.1 Coopération internationale ... 70

2. Principe de la transparence ... 80
2.1 Demandes d'accès ... 80
2.1.1 Départements et offices fédéraux ... 80
2.1.2 Services parlementaires ... 81
2.1.3 Ministère public de la Confédération ... 81
2.1.4 Demandes en médiation ... 81
2.2 Consultations des offices et autres prises de position 83
2.2.1 Introduction du nouveau standard de l'OCDE sur l'échange automatique de renseignements en matière fiscale ... 83
2.2.2 Projet de révision partielle de la loi sur l'aviation ... 84
2.2.3 Révision de la loi fédérale et de l'ordonnance sur les marchés publics ... 85
2.2.4 Révision de l'article 15 de l'Ordonnance sur la transparence ... 86
2.3 Varia ... 88
2.3.1 Évaluation de la loi sur la transparence et participation au groupe d'accompagnement ... 88
2.3.2 Relations avec les préposés cantonaux à la transparence – groupe de travail sur la médiation ... 92

3. Le PFPDT 93
3.1 Neuvième Journée de la protection des données 93
3.2 Publications du PFPDT au cours de l'année sous revue 94
3.3 Statistique des activités du PFPDT du 1er avril 2014 au 31 mars 2015 97
3.4 Statistique des demandes d´accès présentées auprès des départements en vertu de l´art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014) 100
3.5 Statistique des demandes d'accès présentées auprès du Ministère public de la Confédération en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014) 109
3.6 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014) 110
3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2014 au 31 décembre 2014) 111
3.8 Secrétariat du PFPDT 112

Avant-propos

En finir avec le Far West numérique

Ainsi titrait la NZZ dans l'une de ses récentes éditions, en allant à l'essentiel: le débat sur le big data et l'Internet des objets bat son plein et révèle en même temps de graves lacunes en matière de réglementation. C'est un thème qui ne laisse personne indifférent: analystes de tendances, représentants des milieux économiques, scientifiques, éthiciens et autres spécialistes ont en ont analysé les possibilités et les dangers sous ses différents aspects. Alors que les uns critiquent ce qu'ils nomment le Far West numérique et réclament des règles, les autres applaudissent au potentiel économique immense des mégadonnées (big data) et répandent une ambiance de ruée vers l'or. J'ai moi-même participé à de nombreux colloques et vécu de près cette controverse. Les avis sont unanimes au moins sur un point: cette évolution est un très grand défi pour la protection de la sphère privée.

Dans son livre «La nouvelle société du coût marginal zéro», Jeremy Rifkin relève l'énorme potentiel de la révolution numérique avec l'Internet des objets, tout en estimant que «le problème de la sphère privée demeurera une préoccupation majeure qui déterminera dans une large mesure tant le rythme de la transition que les chemins que nous emprunterons dans la prochaine période de notre histoire». Toutefois, les solutions proposées ne pourraient pas être plus différentes. Alors que les uns mettent en garde contre des répercussions majeures, d'autres réclament l'abolition de la sphère privée, arguant que dans l'Antiquité, elle n'existait pas, ce qui signifie en définitive ceci: si nous voulons profiter pleinement du progrès technique, nous devons jeter par-dessus bord les idées héritées de la philosophie des Lumières et nous soumettre à terme à des formes sociales autoritaires – tout comme les esclaves de l'Antiquité! Rifkin emprunte une autre voie et pose une question centrale, à savoir comment garantir, dans ces circonstances, une communication ouverte et transparente tout en assurant que les données d'une personne ne soient pas traitées sans son autorisation et de manière dommageable pour elle?

Qui gagnera cette bataille? Nous en saurons plus dans dix ans. C'est le temps qu'il nous faudra probablement attendre pour que le potentiel de cette évolution technique se déploie pleinement. En effet, l'Internet des objets, le grand fournisseur des mégadonnées du futur, n'en est qu'à ses débuts. Certes, avec le protocole Internet IPv6, les conditions techniques sont réunies pour qu'un nombre illimité d'objets soient munis d'adresses IP, permettant une communication à travers la Toile. Mais la mise en œuvre économique prendra encore du temps. Si nous voulons influencer le cours des choses, les règles doivent être rapidement adaptées, sinon le développement technique nous placera devant le fait accompli.

La question sera aussi de savoir si l'Europe a la volonté de poser des limites au monopole néo-féodal de Google, Facebook, Amazon et consorts. Les premières voix s'élèvent au sein des gouvernements européens qui menacent ces géants mondiaux de mesures antitrust. La Suisse doit elle aussi se positionner face à cette révolution technologique et en peser les avantages et les inconvénients. Nous devons instaurer un débat social profond et mettre en place une stratégie de la société numérique. J'espère vivement que la Commission Rechsteiner, qui doit livrer ses résultats d'ici la fin de l'année 2017, donnera un élan important qui se manifestera également dans la révision de la loi sur la protection des données (LPD).

Après les attentats de Paris et de Copenhague, rien d'étonnant à ce que la nouvelle loi sur le renseignement, qui met à la disposition du Service de renseignement des moyens supplémentaires permettant de récolter des informations, ait aisément franchi l'obstacle parlementaire. Quant à savoir si cette loi devra passer en votation populaire, la question demeure ouverte pour l'instant. Dans le contexte des révélations d'Edward Snowden, nous pouvons nous demander si notre pays marche sur les pas des États-Unis en se dotant d'un «Patriot Act» suisse et ouvre ainsi la voie à une surveillance totale. Toutefois, nous devons ici faire une distinction: aussi sceptique l'on puisse être, il faut souligner que les mesures de surveillance ne pourront être prises que dans des cas concrets, sur mandat de l'autorité judiciaire et avec l'autorisation de la Délégation du Conseil fédéral pour la sécurité. Le conseiller fédéral Ueli Maurer et le Service de renseignement soulignent qu'il ne s'agit que d'une douzaine de cas par an. Il incombe donc au contrôle parlementaire, exercé par la Délégation des Commissions de gestion, de veiller à ce que ce cadre soit respecté.

Même si l'on comprend que la protection de l'État puisse requérir des compétences supplémentaires, le projet soumis au Parlement n'en demeure pas moins quelque peu préoccupant. Surtout parce que les compétences de la protection de l'État vont, pour certaines, plus loin que celles des autorités de poursuite pénale. Contrairement à ces dernières, le Service de renseignement n'a pas besoin de soupçons concrets pour recourir à des mesures de contrainte. Une question, entre autres, reste ouverte: qu'advient-t-il lorsque les services de renseignement se heurtent à des infractions pénales? Il est important de clarifier ce point, d'autant plus que la révision actuellement en cours de la loi sur la surveillance des télécommunications prévoit de doter aussi les autorités de poursuite pénale de moyens supplémentaires, notamment de chevaux de Troie gouvernementaux.

Le numéro AVS continue à se propager en tant qu'identificateur personnel dans différents domaines administratifs en dehors des assurances sociales. Cette année par exemple, il s'agit du Registre du commerce. Nous nous sommes engagés pour qu'à l'instar de la loi sur le dossier électronique du patient (LDEP), la Centrale de

compensation crée un identificateur indépendant de l'AVS. La résistance du Registre du commerce a été en partie vaincue au cours de la procédure de consultation des offices. Le Registre du commerce devra mettre dorénavant en place un identificateur sectoriel issu du numéro AVS et empêchera ainsi une utilisation directe de celui-ci. Nous aurions préféré une solution indépendante du numéro AVS, comme dans le cas du dossier électronique du patient. Nous déplorons aussi que différentes approches aient été ainsi mises en place dans différentes unités administratives. Le Conseil fédéral devrait se pencher sur cette question dans l'optique de parvenir à une pratique uniforme. Il faut prendre une décision de principe sur la licéité de l'utilisation généralisée du numéro AVS en tant qu'identifiant personnel unique, étant donné les risques encourus au niveau des droits fondamentaux.

Les plateformes d'information en matière économique ont aussi constitué pour nous un thème majeur au cours de l'année sous revue, plus précisément la multitude de données que ces plateformes traitent, telle Moneyhouse, bien loin du seul but de vérification de la solvabilité. À la suite de nombreuses plaintes, nous avons examiné de près la pratique de cette entreprise et avons ensuite formulé de nombreuses recommandations. Celles-ci ont été en partie acceptées. Nous allons à présent soumettre les aspects pour lesquels il n'a pas été possible de trouver un accord au Tribunal administratif fédéral afin de clarifier la situation juridique.

Plus positivement, mentionnons l'évolution observée dans le secteur de la santé. Dans le cadre de l'introduction des montants forfaitaires par cas (le système SwissDRG) et de l'augmentation des flux de données qui en découle, nous avons obtenu que le tri des factures numérisées soit fait conformément aux exigences de la protection des données, au sein des assurances-maladie, par des services de réception des données indépendants et certifiés placés sous la surveillance du PFPDT. Depuis leur création, nous avons contrôlé de nombreux services de réception des données et mis au point des directives. Aujourd'hui, nous sommes en mesure de constater que ce nouveau concept a été mis en œuvre selon nos attentes et que cela contribue considérablement à ce que les flux de données dans le domaine de la santé soient régulés et gérés selon des critères uniformes.

Actuellement, la tendance est à la délocalisation de services dans le nuage. A ce propos, régulièrement, des organes de la Confédération nous demandent s'ils peuvent confier des traitements de données à des fournisseurs étrangers. Nous avons fermement rappelé qu'il leur incombe de gérer avec une grande circonspection les données personnelles des citoyens et de les protéger d'un accès non autorisé par des autorités étrangères. Il convient donc en général de renoncer à ce type de délocalisation. Mais pour les particuliers aussi, il est de en plus difficile d'utiliser des appareils sans recourir aux traitements dans le nuage. Jusqu'ici, les appareils mobiles pouvaient être sécurisés ou synchronisés localement. Les produits de

dernière génération obligent l'utilisateur à transférer ses données personnelles vers des centres de données inconnus. Les fabricants mettent ainsi les utilisateurs sous tutelle et en définitive leur ôtent le contrôle de leurs propres données.

Le 16 avril 2014, le Conseil fédéral a adopté la stratégie de libre accès aux données publiques en Suisse pour la période 2014-2018. Cette décision a incité les milieux concernés à poser au Conseil fédéral des questions sur le potentiel économique d'une utilisation novatrice des données dans les domaines de l'énergie, des transports et de la santé, ainsi que sur le positionnement de la Suisse dans la course mondiale aux données. De notre point de vue, il est important que le Conseil fédéral ait souligné dans sa réponse qu'il entendait examiner d'ici à la fin de l'année les champs d'action prioritaires dans le domaine des mégadonnées, notamment en ce qui concerne la protection des données et le droit à disposer de ses données personnelles. Nous allons suivre attentivement cette question, aussi et surtout dans la perspective de la révision de la LPD.

Dans le contexte du principe de transparence dans l'administration, l'on mentionnera l'arrêt déterminant du Tribunal administratif fédéral qui a appuyé notre recommandation concernant la Commission pour la technologie et l'innovation. Le Tribunal a conclu que le public a un intérêt majeur à savoir comment les deniers publics sont utilisés dans le contexte de la promotion de l'innovation. Il y a un an, j'avais exprimé la crainte que l'évaluation concernant la loi sur la transparence (LTrans) puisse se transformer en invitation à affaiblir la loi. Cela surtout parce que l'initiative de l'évaluation avait été prise par certains offices qui considèrent que cette loi entrave leur action. Ce rapport est maintenant disponible. Il est analysé en détail au chapitre 2.4.1. Relevons avant tout un sujet de satisfaction pour nous: la procédure de médiation telle que nous la pratiquons a été très bien acceptée et ce malgré le fait que dans la plupart des cas, nous n'avons pas pu tenir les délais par manque de ressources. Par ailleurs, ce rapport n'offre aucun tremplin à un affaiblissement de la loi. Au contraire, il est important de constater que le changement de paradigme requis par la LTrans n'est toujours pas concrétisé dans toute l'administration fédérale. Toutefois, nous voudrions souligner que cette loi est de mieux en mieux acceptée, surtout là où la mise en œuvre de la LTrans est soutenue à l'échelon hiérarchique supérieur. Les nombreux arrêts du Tribunal administratif fédéral et du Tribunal fédéral qui, dans la plupart des cas, ont soutenu les recommandations du PFPDT y sont aussi pour quelque chose.

.

Liste des abréviations

AFC	Administration fédérale des contributions
ATF	Arrêt du tribunal fédéral
CDF	Conférence des directrices et directeurs cantonaux des finances
CDF	Contrôle fédéral des finances
CEDH	Convention européenne des droits de l'homme
CF	Conseil fédéral
CFF	Chemins de fer fédéraux suisses
ChF	Chancellerie fédérale
CP	Code pénal suisse
CSI	Conférence suisse sur l'informatique
DDPS	Département fédéral de la défense, de la protection de la population
et des sports	
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DRG	Diagnoses Related Groups
fedpol	Office fédéral de la police
FF	Feuille fédérale
FINMA	Autorité fédérale de surveillance des marchés financiers
GTID	Groupe de Travail Interdépartemental
ISAS	Système d'information pour la sécurité extérieure
ISIS	Système d'information pour la sécurité intérieure
JANUS	Système informatisé de la Police judiciaire fédérale
LA	loi fédérale sur l'aviation
LAAM	Loi fédérale sur l'armée et l'administration militaire
LAGH	Loi fédérale sur l'analyse génétique humaine
LAMal	Loi fédérale sur l'assurance-maladie
LDEIP	Loi fédérale sur le dossier électronique du patient
LFRC	Loi fédérale sur le renseignement civil
LJAr	Loi fédérale sur les jeux d'argent
LLP	Loi fédérale sur les loteries et les paris professionnels
LMJ	Loi sur les maisons de jeu

LMP	Loi fédérale sur les marchés publics
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LPD	Loi fédérale sur la protection des données
LPMA	loi fédérale sur la procréation médicalement assistée
LRCS	Loi fédérale relative à la recherche sur les cellules souches embryonnaires
LRH	Loi fédérale relative à la recherche sur l'être humain
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LSIP	Loi fédérale sur les systèmes d'information de police de la Confédération
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
LTV	Loi sur le transport de voyageurs
MARS	Modules ambulatoires des relevés sur la santé
NIF	Numéro d'identification fiscale
OAMal	Ordonnance sur l'assurance-maladie
OCDE	Organisation de Coopération et de Développement Économiques
ODM	Office fédéral des migrations (SEM depuis le 1er janvier 2015)
OFAC	Office fédéral de l'aviation civile
OFAS	Office fédéral des assurances sociales
OFE	Office fédéral de l'énergie
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFRC	Office fédéral du registre du commerce
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFSPO	Office fédéral du sport
OFT	Office fédéral des transports
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
OMP	Ordonnance sur les marchés publics
OSI-SRC	Ordonnance sur les systèmes d'informations du Service de renseignement de la Confédération

OTrans	Ordonnance sur le principe de la transparence dans la Confédération
PFPDT	Préposé fédéral à la protection des données et à la transparence
SAS	Service d'accréditation suisse
SEM	Secrétariat d'État aux migrations (jusqu'au 31.12.2014: Office fédéral des migrations, ODM)
SFI	Secrétariat d'État aux questions financières internationales
SGPD	Système de gestion de protection des données
SIPD	Sûreté de l'information et de protection des données
SIS	Système d'information Schengen
SIS II	Système d'information de Schengen II
SIS II SCG	groupe de coordination du contrôle du SIS II
SRC	Service de renseignement de la Confédération
SRD	Service de réception des données
TAF	Tribunal administratif fédéral
TIC	Technologies de l'information et de la communication
UPI	Unique Personal Identifier Database
UPIC	Unité de pilotage informatique de la Confédération
Zefix	Index central des raisons de commerce

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Nouvelles directives sur la certification

Les nouvelles normes ISO 27001 et ISO 27002 étant entrées en vigueur en automne 2013, nous avons procédé au printemps 2014 à l'adaptation de nos directives sur la certification ainsi qu'à celle de leur annexe.

Les normes ISO/CEI 27001/2:2013 concernant les systèmes de management de la sécurité de l'information ont été entièrement révisées et sont entrées en vigueur le 1er octobre 2013. Comme notre référentiel de certification se base fortement sur ces deux normes internationales, il a été nécessaire d'adapter en conséquence nos Directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir, ainsi que leur annexe.

Les modifications structurelles d'ISO 27001 («Exigences») portent pour l'essentiel sur un alignement avec l'annexe SL du Supplément ISO consolidé des Directives ISO/CEI. Nos nouvelles directives, entrées en vigueur le 1er mai 2014, mettent notamment à jour les définitions conformément à la norme ISO/CEI 27000:2014. En outre, une disposition transitoire a permis aux procédures de certification en cours d'être achevées sous l'ancien régime jusqu'au 1er octobre 2014.

La norme ISO 27002 («Code de bonne pratique») a par contre subi une refonte plus en profondeur, avec l'introduction de nouveaux chapitres dédiés à la cryptographie et aux relations avec les fournisseurs, et avec la séparation de la sécurité de l'exploitation de celle des communications. Au total, la norme compte désormais 18 chapitres comprenant un ensemble de 114 mesures. Tous ces changements se répercutent sur l'annexe à nos directives appelée «Code de bonne pratique pour la gestion de la protection des données». L'annexe réaligne les mesures de mise en œuvre pour la sécurité des données, en ajoutant en ce qui concerne la confidentialité les nouvelles mesures prévues pour la sécurité de l'information dans la gestion de projet, pour les appareils mobiles et le télétravail, ainsi que pour la cryptographie. Au final, l'annexe comporte toujours neuf objectifs comprenant 20 mesures, dont celles consacrées à la sécurité des données renvoient désormais à 71 mesures de la nouvelle norme ISO 27002.

Les actuels organismes de certification accrédités par le SAS nous ont confirmé a posteriori que la transition s'était bien déroulée, en particulier dans le cadre des services de réception des données (SRD).

1.1.2 Modifications du code civil – Infostar et registre foncier

Dorénavant, la Confédération portera l'entière responsabilité de l'exploitation du registre électronique de l'état civil (Infostar). En outre, le numéro AVS sera introduit dans le registre foncier à titre d'identificateur de personne, permettant ainsi une recherche de biens-fonds sur l'ensemble du pays. Nous nous sommes prononcés au sujet de ces modifications au cours de la procédure de consultation. Le Conseil fédéral n'a pas accepté notre proposition de créer un identifiant sectoriel des personnes.

Étant donné le rôle majeur d'Infostar en tant que système central d'informations personnelles, nous avons proposé à l'Office fédéral de la justice, dans le cadre de la consultation des offices, de régler tous les aspects du registre au niveau législatif. La création d'un entrepôt de données comme banque de données miroir d'Infostar, destiné à assurer la surveillance de la qualité, nous a semblé insuffisamment réglementée dans le projet.

Par ailleurs, nous avons à nouveau jugé l'introduction du numéro AVS dans le registre foncier disproportionnée (cf. notre 20e rapport d'activités 2012/2013, ch. 1.5.1). Nous avons répété clairement notre position concernant l'utilisation de ce numéro comme identifiant personnel universel. Le Conseil fédéral n'a malheureusement pas suivi notre proposition d'introduire un identifiant sectoriel similaire à celui que prévoit la loi fédérale sur le dossier électronique du patient (cf. notre 21e rapport d'activités 2013/2014, ch. 1.5.1). Nous suivons avec attention l'évolution tendant à introduire le numéro AVS comme identifiant personnel universel dans toute l'administration et même au-delà.

1.1.3 Révision de la loi sur le registre du commerce

Nous nous sommes à nouveau exprimés sur la révision de la loi sur le registre du commerce au cours de l'année sous revue. Nous avons fait état de nos préoccupations concernant l'utilisation du numéro AVS et l'absence de «droit à l'oubli». Dorénavant, les offices des registres du commerce ont la possibilité de demander un émolument en cas de demande d'accès à des documents. Cet obstacle financier a pour but d'entraver les demandes disproportionnées.

Dans nos deux derniers rapports d'activités (2012/2013 et 2013/2014, ch. 1.8.4), nous avons abordé les aspects du projet de loi relatifs à la protection des données. Au cours de l'année sous revue, nous nous sommes également prononcés sur la révision du droit du registre du commerce.

Il est toujours possible de comparer les données personnelles générées lorsqu'on s'annonce à un registre du commerce via la base de données UPI auprès de la Caisse de compensation. Celle-ci gère dans cette base de données les données personnelles appartenant au numéro AVS. Cette comparaison a pour but d'améliorer la qualité des données dans le registre du commerce et, entre autres, de trouver et fusionner les entrées en double ou triple exemplaire au sujet d'une personne. Dans le projet, le nombre des services qui ont accès aux numéros AVS a désormais été réduit. En outre, il est prévu dans la loi elle-même que les numéros AVS ne soient pas publiquement accessibles. Enfin, un identifiant sectoriel, que l'on ne peut relier au numéro AVS, doit être créé pour les personnes physiques.

Désormais, les offices des registres du commerce pourront exiger le paiement d'une taxe pour la consultation de documents qui contiennent notamment des données personnelles sensibles. Cet obstacle financier a pour but de réduire les demandes de consultation. En outre, les demandeurs doivent s'identifier au moment de payer, ce qui devrait empêcher les demandes de consultation abusives.

Dans notre prise de position, nous avions attiré l'attention de l'Office fédéral du registre du commerce (OFRC) sur le jugement rendu par la Cour de justice de l'Union européenne concernant le droit à l'oubli: Dans son jugement du 13 mai 2014, celle-ci a établi que les moteurs de recherche sont responsables du traitement des données personnelles apparaissant sur leurs pages Internet et qu'ils doivent, à certaines conditions et sur demande des personnes concernées, supprimer certains liens. Si au départ, il avait été prévu d'introduire un droit à l'oubli, à l'occasion de la révision de loi, cette mesure a ensuite été abandonnée en raison du manque d'intérêt des participants à la consultation. Selon l'OFRC, le site www.zefix.ch n'est pas visé par la décision de la Cour de justice de l'Union européenne; de plus, il estime que cette décision s'adresse aux exploitants de moteurs de recherche et relève que le site www.zefix.ch n'est pas indexé par un moteur de recherche. Toutefois, un certain nombre des demandes que nous avions émises ont été reprises par l'OFRC, ce qui a permis de renforcer la protection de la personnalité.

1.1.4 Projet de loi fédérale relative à l'application des principes du débiteur et de l'agent payeur à l'impôt anticipé

Au cours de la consultation des offices concernant le projet de loi fédérale relative à l'application des principes du débiteur et de l'agent payeur, nous nous sommes prononcés contre l'introduction du numéro AVS comme identificateur pour les personnes physiques. Notre intervention a rencontré un succès partiel. Le Conseil fédéral décidera ultérieurement si le numéro AVS ou un identifiant personnel sectoriel sera utilisé.

L'impôt anticipé repose actuellement sur le principe du débiteur et porte exclusivement sur les revenus de source de production nationale. Est soumis à cet impôt le débiteur situé sur le territoire suisse, par exemple l'entreprise dont le siège est en Suisse et qui émet un titre obligataire sur lequel elle verse un intérêt aux investisseurs. L'impôt est perçu indépendamment de la personne du créancier et concerne donc notamment les investisseurs institutionnels. Avec le changement de système, le Département fédéral des finances (DFF) entend parer efficacement aux inconvénients inhérents au système actuel. Désormais, l'impôt anticipé ne sera plus perçu par le débiteur, mais par l'agent payeur suisse (une banque) qui créditera les revenus correspondants à son client.

Dans le projet de loi, il était initialement prévu que dans la déclaration à l'Administration fédérale de contributions (AFC), les agents payeurs soient obligés de communiquer le numéro AVS ou le numéro d'identification de l'entreprise (IDE). Cela aurait encore plus élargi le cercle des services autorisés à utiliser systématiquement le numéro AVS. Dans le présent rapport d'activités (cf. notamment ch. 1.1.3 et 1.1.7), nous avons abordé les risques que comporte pour la protection de la personnalité l'utilisation dans l'administration d'un seul identifiant personnel. Nous avons donc pris position dans ce sens et demandé la création d'un identifiant personnel sectoriel pour le domaine fiscal. Le projet a été ensuite modifié et il a été proposé au Conseil fédéral de décider ultérieurement si le numéro AVS ou un identifiant sectoriel sera utilisé dans le domaine fiscal. À nos yeux, cette proposition au Conseil fédéral va trop loin. Le Conseil fédéral a certes pris connaissance des préoccupations présentées dans notre rapport, mais il s'est prononcé contre notre requête.

1.1.5 Projet MARS de l'Office fédéral de la statistique et de l'Office fédéral de la santé publique

Nous continuons à suivre l'évolution du projet MARS (Modules ambulatoires des relevés sur la santé). La modification en cours de l'ordonnance sur l'assurance-maladie devrait permettre de régler les détails du traitement des données. Un règlement de traitement est également en cours d'élaboration.

L'Office fédéral de la statistique (OFS) est chargé par la loi sur la statistique fédérale de produire des statistiques d'intérêt public. Dans le domaine de la santé, l'OFS a pour mission spécifique d'établir les bases statistiques nécessaires à l'examen du fonctionnement et des effets de la loi fédérale sur l'assurance-maladie (LAMal). Il faut pour cela étendre les relevés statistiques fédéraux à la médecine ambulatoire, afin d'obtenir des données sur l'ampleur des soins ambulatoires, sur les raisons du recours à ces soins (diagnostics) ainsi que sur les prestations et sur les coûts du

secteur ambulatoire. L'OFS effectue également, en vertu de la LAMal, des relevés auprès des fournisseurs de prestations afin de pouvoir transmettre des données aux instances qui sont chargées d'une mission légale de surveillance.

Conformément à l'art. 22a al. 4 LAMal, le Conseil fédéral doit encore régler les détails de la collecte, du traitement, de la transmission et de la publication des données, dans le respect du principe de la proportionnalité. Nous avons rappelé ce point dans un courrier aux directions de l'Office fédéral de la santé publique (OFSP) et de l'OFS. Nous les avons également rendus attentifs à la nécessité d'élaborer le plus rapidement possible un règlement de traitement abordant en détails l'utilisation du numéro AVS, les appariements de données, la pseudonymisation et l'anonymisation, ainsi que le procédé cryptologique et le Key Management.

Lors de l'assemblée de la chambre médicale de la FMH en mai 2014, nous sommes également intervenus publiquement en insistant sur la nécessité d'une concrétisation rapide de l'art. 22a al. 4 LAMal. Au vu de la nature sensible des données personnelles collectées, nous restons particulièrement attentifs au développement du projet et veillons à ce que les exigences de la protection des données soient pleinement respectées.

1.1.6 Échange de données personnelles entre les registres des habitants, la Poste et d'autres détenteurs de données

Nous avons participé aux travaux de réflexion sur l'échange de données personnelles entre les contrôles des habitants, la Poste et d'autres détenteurs de données. Le Conseil fédéral a abandonné l'idée d'un échange automatique d'adresses entre la Poste et les registres des habitants. Il a, en revanche, chargé le Département fédéral de justice et police d'examiner de plus près les solutions permettant un échange automatique d'adresses entre les différents organes publics.

En date du 12 novembre 2014, le Conseil fédéral a élaboré un rapport en exécution du postulat 12.3661 de la Commission des institutions politiques du Conseil national («Échange de données personnelles entre les registres des habitants, la Poste et d'autres détenteurs de données»), lancé en réaction à l'initiative parlementaire 11.488 du 29 septembre 2011. Le Conseil fédéral était chargé de déterminer s'il y a lieu de créer des bases légales visant à mettre en place un échange automatique et régulier des adresses entre différents détenteurs de données publics, notamment La Poste Suisse et les contrôles des habitants.

Sur la base des travaux menés au sein du groupe de travail auquel nous avons participé, le Conseil fédéral est parvenu à la conclusion qu'il n'était pas judicieux d'instaurer un tel échange automatique. Les listes d'adresses des registres des habitants sont déjà de très bonne qualité et le fait d'introduire un échange automatique et régulier de données personnelles entre La Poste suisse et les services de contrôle des habitants poserait des problèmes de protection des données. En effet, la transmission de ces données implique l'utilisation d'un identificateur univoque – le numéro AVS. La Poste risquerait de le transmettre aux autres entreprises de distribution, ce qui accroîtrait les risques d'abus. Le système serait dans l'intérêt de La Poste qui deviendrait la seule institution du pays à détenir une banque de données à jour des adresses de tous les habitants.

Un fichier d'adresses serait cependant extrêmement utile aux administrations publiques de tous les échelons de l'État, qui ont besoin, dans pratiquement toutes leurs activités, d'identifier clairement leurs administrés et de connaître leur domicile. Au niveau des communes, ces données sont disponibles dans le registre des habitants, qui est mis à jour de manière permanente. Elles sont aussi généralement accessibles au niveau cantonal. C'est seulement au niveau intercantonal et fédéral qu'elles font défaut. Les administrations sont contraintes de renoncer à actualiser les données dont elles disposent ou de les obtenir des communes et des cantons, au cas par cas, ce qui complique nettement nombre de processus administratifs. On peut citer comme exemples la perception de la taxe d'exemption de l'obligation de servir, le paiement des primes d'assurance-maladie, ou les procédures de poursuite, si le débiteur déménage dans un autre canton. Ces difficultés pourraient être évitées et les processus administratifs considérablement simplifiés s'il existait au niveau national une banque fiable de données d'adresses.

Plusieurs solutions sont envisageables. D'abord, la qualité des données d'adresses dans les registres des habitants pourrait être améliorée si tous les cantons veillaient à ce que les bailleurs et les logeurs signalent les personnes qui n'ont pas rempli leur obligation de s'annoncer au service des habitants. En outre, on pourrait créer une banque des données d'adresses à laquelle les administrations publiques pourraient accéder pour accomplir leurs tâches. Cette banque de données pourrait être alimentée par les plateformes cantonales existantes, ou bien se fonder sur des plateformes de la Confédération (la banque de données de l'Office fédéral de la statistique; un répertoire national des personnes, qui serait alors à créer; une extension de la banque de données UPI (Unique Personal Identifier Database) qui sert à la Centrale de compensation).

Le Département fédéral de justice et police est chargé par le Conseil fédéral d'étudier de manière approfondie les avantages et les inconvénients de ces options et notamment leur faisabilité, leur compatibilité avec la protection des données, leur

coût et leurs conséquences. En tant que membre du groupe de travail, nous suivons de près les développements afin de garantir un traitement conforme au droit de la protection des données.

1.1.7 Utilisation d'un identificateur universel de personnes dans la cyberadministration

Nous avons participé à un groupe de travail chargé d'examiner pour le Conseil fédéral la question de l'élaboration de bases légales pour l'utilisation d'un identifiant personnel administratif dans la cyberadministration. Dans ce cadre, nous avons exposé nos craintes quant à l'utilisation généralisée d'un identificateur unique et universel tel que le numéro AVS.

En janvier 2014, la Conférence des directrices et directeurs cantonaux des finances (CDF) a, sur proposition du Comité directeur de la Conférence suisse sur l'informatique (CSI), demandé à la Conseillère fédérale Eveline Widmer-Schlumpf d'examiner la question de la mise en place de bases légales permettant l'introduction d'un identifiant personnel administratif clair et universel, idéalement sur la base du numéro AVS. Selon la CSI, il est nécessaire, pour l'échange électronique de données personnelles entre les systèmes d'informations, et donc pour toutes les applications de cyberadministration, que les données puissent être adressées à l'aide d'un identificateur clair pour chaque personne concernée. Le numéro AVS serait un identifiant possible qui aurait l'avantage, d'une part, d'être attribué à chaque personne résidant en Suisse et, d'autre part, de ne pas permettre de déduction quant à la personne concernée, du fait de sa composition aléatoire. La CDF préconise par ailleurs une certaine souplesse législative pour une utilisation simplifiée du numéro AVS dans tout le domaine de la cyberadministration.

La Conseillère fédérale a admis que cette thématique devait être soumise au Conseil fédéral et a donc chargé l'Unité de pilotage informatique de la Confédération (UPIC) de constituer un groupe de travail en vue d'élaborer un document sur la base duquel le Conseil fédéral sera à même de décider de la marche à suivre. Nous avons avons exposé nos craintes quant à l'utilisation généralisée d'un identificateur unique et universel tel que le numéro AVS dans le cadre de la cyberadministration, compte tenu des risques majeurs qu'il comporte pour la sphère privée des personnes concernées. Une alternative peu coûteuse fiable et facile à mettre en œuvre peut être trouvée dans la mise en place d'un numéro sectoriel tel qu'envisagé pour le dossier électronique du patient.

Outre la base légale à élaborer, il faut également se poser la question de la nécessité et de la proportionnalité d'une utilisation du numéro AVS en dehors du secteur

des assurances sociales. Par ailleurs, le citoyen doit savoir très clairement quels services et institutions se servent systématiquement du numéro AVS en dehors du domaine des assurances sociales. Il convient d'élaborer à cet égard une base légale au sens formel précisant le but de l'utilisation et les utilisateurs légitimés. Nous redoutons que l'utilisation du numéro AVS ne se propage au secteur privé en dehors d'un cadre légal clair et défini. Il ne serait plus possible d'en maîtriser le traitement et de vérifier la légitimité de ce dernier.

1.2 Protection des données – Questions d'ordre général

1.2.1 Révision totale des systèmes d'information de la Confédération dans le domaine du sport

Dans le cadre de la consultation des offices concernant la révision totale de la loi sur les systèmes d'information de la Confédération dans le domaine du sport, nous avons pris position sur la loi et le message. Nous nous sommes notamment exprimés sur la communication de données dans le cadre du Système d'information national pour le sport et du Système d'information pour les résultats du diagnostic de performance.

La loi fédérale sur les systèmes d'information de la Confédération dans le domaine du sport, entrée en vigueur en octobre 2012, a fait l'objet d'une révision totale. Il est notamment question d'ancrer formellement le système d'information de la Haute école fédérale de sport dans la loi car il contient entre autres des données relatives à des procédures disciplinaires. Dans le cadre de la révision, on a également tenu compte des expériences réalisées avec l'application de la nouvelle loi introduite en 2012 et, outre le système d'information évoqué, créé des bases légales formelles pour trois autres systèmes déjà opérationnels ou en cours de développement. Il s'agit d'un système d'information pour le traitement de données relatives aux résultats du diagnostic de performance, d'un système permettant l'évaluation des cours et des formations et d'un système d'information de l'agence nationale de lutte contre le dopage.

La loi prévoit pour le système d'information national pour le sport une communication régulière mais limitée de données personnelles à différents services et personnes. Les modifications ont permis d'ancrer dans la loi une collaboration qui existait déjà en pratique en matière d'équité et de sécurité du sport (p. ex. programme de prévention «cool and clean» ou organisation de sauvetage aérien REGA). Il existe désormais une restriction explicite dans la loi, selon laquelle les données ne peuvent être utilisées à des fins commerciales. Nous avons proposé à l'Office fédéral du sport (OFSPO) que les personnes enregistrées dans le système d'information national pour le sport soient protégées contre les transmissions abusives par les destinataires des données et que l'Office fédéral conserve le contrôle des destinataires de listes et de données électroniques. L'OFSPO oblige déjà les destinataires des données à ne pas communiquer ces dernières. L'Office a donc accepté notre proposition et explicitement interdit la transmission des données par les destinataires dans les dispositions légales.

Concernant le système d'information pour le traitement de données relatives aux résultats du diagnostic de performance, la loi prévoit par ailleurs que les données

et résultats peuvent notamment être communiqués à des personnes, autorités et organisations ayant mandaté les tests et examens. Pour cette communication, aucune autorisation explicite de la part des personnes concernées n'est prévue. Les sportifs concernés sont convoqués par des organisations ou autorités pour les tests du diagnostic de performance et sont informés par les responsables (entraîneurs, médecins de fédération) sur le traitement des données, en particulier sur la finalité des tests, sur l'analyse réalisée ensuite par les spécialistes responsables et sur les destinataires des résultats. La LPD s'applique au traitement ultérieur des données par les destinataires, en particulier les principes de finalité et de proportionnalité.

Le déroulement des tests du diagnostic de performance n'ayant pas été précisé dans le projet de message, le risque existait selon nous qu'on ne puisse comprendre, sans connaissance supplémentaire des processus, pourquoi la loi n'exige dans ce cas aucune autorisation pour la transmission des données. Nous avons donc suggéré de compléter le message avec des explications sur la communication des données aux destinataires. L'OFSPO a répondu favorablement à notre demande et complété le message dans ce sens.

1.2.2 Système d'information concernant les voyageurs sans titre de transport valable

La nouvelle base légale pour un système d'information sur les voyageurs sans titre de transport valable a été adoptée par le Parlement. Les dispositions d'exécution correspondantes sont en cours d'élaboration.

En vue de la création d'une base légale pour des systèmes d'information relatifs aux voyageurs sans titre de transport valable, l'Office fédéral des transports (OFT) a élaboré une nouvelle disposition dans la loi sur le transport de voyageurs (LTV) (voir à ce sujet notre 21e rapport d'activités 2013/2014, chiff. 1.2.6). Cette nouvelle disposition (art. 20a LTV) a été approuvée sous une forme légèrement modifiée après été débattu par le Parlement dans le cadre du paquet législatif «Loi sur les entreprises de transport par route et loi du droit pénal des transports. Modification». Le Parlement y a ajouté un nouvel alinéa selon lequel les systèmes d'information peuvent également être exploités par l'association faîtière du secteur.

Le texte de la loi prévoit que les entreprises de transport concessionnaires peuvent exploiter des systèmes d'information sur les voyageurs sans titre de transport valable, et règle certains points tels que la suppression des données. L'OFT travaille actuellement sur les dispositions d'exécution. Les entreprises concessionnaires, et/ou le cas échéant l'association faîtière, devront régler de manière détaillée l'organisation concrète des systèmes d'information au travers de directives, de règlements de traitement ou sous toute autre forme appropriée.

1.2.3 Stockage centralisé des photos de clients dans les stations de ski – explications générales

Nous avons publié des explications sur la manière dont les systèmes de contrôle d'accès utilisés par la plupart des stations de ski en Suisse peuvent être configurés et exploités.

Après avoir clos la procédure d'examen des faits que nous avons menée dans une station de ski au cours de l'année précédente (cf. le 21e rapport d'activités 2013/2014, ch. 1.2.1), nous avons rédigé des explications générales sur la manière dont les systèmes de contrôle d'accès utilisés par la plupart des stations de ski suisses peuvent être configurés et exploités dans le respect des principes de la protection des données. Nous y précisons en particulier quelles données peuvent être conservées combien de temps, à quelles fins elles peuvent être utilisées, qui peut y avoir accès et comment informer correctement les clients. Ces explications peuvent être consultées sur notre site Internet www.leprepose.ch ¬– Protection des données – Loisirs et sport – Systèmes de contrôle – Exploitation des systèmes d'accès dans les centres de loisirs.

1.2.4 Surveillance vidéo dans les véhicules

L'utilisation des «caméras embarquées» (dashcams) contrevient en général au droit de la protection des données. C'est pourquoi ces caméras ne devraient pas être utilisées. Nous avons publié des explications à ce sujet.

Un accident de voiture est vite arrivé et souvent, il n'est pas facile de constater a posteriori qui a provoqué l'accident. Pour cette raison, des caméras sont de plus en plus souvent installées dans les véhicules. Ces caméras filment la route devant le véhicule (et parfois aussi à l'arrière du véhicule) afin de produire des preuves utilisables en cas d'accident. Dans certains pays, l'utilisation de ces caméras est imposée par la loi, celles-ci connaissent chez nous aussi un engouement croissant. Outre leur utilisation comme moyen de preuve, les enregistrements de caméras embarquées sont aussi mises en ligne sur des réseaux sociaux ou des sites de partage de vidéos, ou même diffusés par les médias à des fins d'information, comme cela a été le cas pour l'accident de transport d'une excavatrice sur l'autoroute A1, que tout le pays a pu regarder.

Même si ces types d'enregistrements peuvent avoir une certaine utilité, ils n'en demeurent pas moins problématiques du point de vue de la protection des données. En général, une caméra embarquée filme en continu. De ce fait, le traitement de données ne se limite pas aux personnes qui sont impliquées dans l'événement (par exemple un accident) ou se comportent de manière fautive, mais concerne

toutes les personnes présentes dans le champ de la caméra. De plus, les personnes concernées ne savent pas qu'elles sont filmées. De ce fait, l'utilisation de caméras embarquées est contraire aux principes de transparence et de proportionnalité. Elle est susceptible de constituer une atteinte illicite aux droits de la personnalité, sans mentionner le fait que souvent, les enregistrements ne sont pas acceptés comme moyens de preuve.

La situation est autre lorsque la caméra est enclenchée uniquement lorsque survient un accident: dans ce cas, tous les utilisateurs de la route ne sont pas considérés comme des suspects potentiels et il n'y a pas de traitement de données à titre préventif. Si l'enregistrement est limité à un événement concret, le traitement de données peut être justifié par un intérêt prépondérant.

Pour plus de précisions à ce sujet, il est possible de consulter nos «Explications sur la vidéosurveillance au moyen de caméras embarquées», sur notre site Internet: www.leprepose.ch, Protection des données – Technologies – Vidéosurveillance.

1.2.5 Nouvelle loi sur les jeux d'argent

Conformément au projet de nouvelle loi sur les jeux d'argent, les jeux en ligne aussi seront à l'avenir autorisés en Suisse. Dans ce contexte, nous nous sommes exprimés sur les listes noires et sur les problèmes d'authentification.

Nous nous sommes exprimés au sujet de l'avant-projet de loi fédérale sur les jeux d'argent (LJAr), destinée à remplacer à la fois la loi sur les maisons de jeux (LMJ) et la loi fédérale sur les loteries et les paris professionnels (LLP). Outre diverses nouveautés proposées concernant l'organisation des autorités compétentes, la nouvelle loi autorise l'organisation des jeux d'argent en ligne. Un certain nombre de problèmes se posent dans ce contexte quant à la vérification des renseignements fournis par les joueurs au moment de l'ouverture d'un compte d'utilisateur.

Du point de vue du droit de la protection des données, l'affichage d'une page STOP destinées aux joueurs cherchant à accéder aux offres étrangères bloquées, l'analyse de ces accès et l'établissement des listes noires étaient en soi problématiques. À la suite de notre prise de position, nous avons évoqué nos préoccupations avec les spécialistes compétents de l'Office fédéral de la justice. La consultation sur la nouvelle loi sur les jeux d'argent a pris fin en août 2014; nous continuons à suivre avec attention les travaux législatifs.

1.3 Internet et télécommunication

1.3.1 Externalisation dans le nuage du traitement des données par les organes fédéraux

Les organes fédéraux prévoient de plus en plus d'externaliser le traitement des données dans le nuage. Les services compétents nous ont contactés pendant l'année sous revue et nous ont demandé de nous prononcer sous l'angle de la protection des données.

Si des autorités fédérales souhaitent externaliser des traitements de données, le droit de la protection des données leur impose de veiller à plusieurs points en plus des conditions générales pour le traitement des données:

- selon la loi sur la protection des données, elles ne doivent transmettre des données personnelles à des tiers que s'il existe une base légale pour ce faire au sens de l'art. 17 LPD, ou si une disposition d'exception au sens de l'art. 19 al. 1 LPD s'applique.
- S'il existe une obligation légale ou contractuelle de garder le secret, les données ne doivent pas être confiées à un prestataire d'informatique en nuage (cloud computing). Il est ainsi également envisageable que seule une partie du traitement des données puisse être externalisée.
- Le maître de fichier doit s'assurer que le mandataire n'effectue le traitement de données que de la manière dont il serait lui-même en droit d'effectuer. Il incombe à l'organe fédéral de vérifier régulièrement le respect des contrats de traitement des données.
- Si les serveurs du prestataire se trouvent à l'étranger, il convient également de respecter les dispositions de protection des données dans le cadre du transfert transfrontalier. La transmission à l'étranger de données personnelles des visiteurs de site Internet peut notamment permettre aux autorités étrangères d'accéder aux données situées dans leur pays, sur la base de leur législation nationale. Vu leur devoir de diligence, ce point se révèle particulièrement délicat pour les offices fédéraux, qui doivent protéger les citoyens notamment contre les accès non autorisés.

Nous critiquons le manque de contrôle sur le mandataire assurant le traitement des données. Par exemple, un long délai de conservation des données n'est pas proportionné et ne correspond pas aux exigences de la LPD. Les prestataires n'autorisant généralement pas d'adaptation de leurs clauses contractuelles standard, l'organe fédéral responsable doit évaluer si un recours aux prestations aux conditions convenues est envisageable ou non.

Il convient de bien évaluer les risques liés à une externalisation lorsque des entreprises américaines sont précisément choisies en tant que prestataires. Ainsi, le 25 avril 2014, le tribunal du Southern District of New York a émis un jugement sensible concernant l'accès des autorités américaines aux données clients stockées au sein de l'UE. Selon ce dernier, les autorités américaines peuvent accéder aux données qui sont traitées dans le cadre d'un mandat par des entreprises ayant leur siège aux États-Unis. Nous partons de l'idée que les applications en nuage d'entreprises américaines peuvent donc permettre aux autorités américaines d'accéder aux données clients stockées sur des serveurs dans l'Union européenne ou en Suisse sans avoir à recourir à l'entraide judiciaire internationale, même si une convention complémentaire est prévue.

Pour ces raisons, nous déconseillons aux organes fédéraux d'externaliser le traitement des données à des entreprises soumises à une législation n'offrant pas un niveau approprié de protection des données. Par ailleurs, il est à noter que les traitements de données à externaliser peuvent concerner des infrastructures d'importance vitale qui, selon les prescriptions du Conseil fédéral, ne peuvent être confiées qu'à des entreprises «soumises exclusivement au droit suisse, détenues en majorité par des propriétaires suisses et fournissant toutes leurs prestations sur le territoire suisse».

1.3.2 Révision partielle de la loi fédérale sur la radio et la télévision – utilisation des numéros AVS par Billag

Les Chambres fédérales ont approuvé la révision partielle de la loi sur la radio et la télévision, qui prévoit un registre national de toutes les personnes enregistrées en Suisse avec leur numéro AVS. De notre point de vue, ce traitement de données n'est pas nécessaire, et nous le jugeons par conséquent disproportionné.

En septembre 2014, le Parlement a approuvé la révision partielle de la loi sur la radio et la télévision. Malheureusement, notre demande de renoncer à l'utilisation des numéros AVS pour la perception des redevances n'a pas été prise en compte par les Chambres, comme l'OFCOM auparavant. Nous continuons de penser que l'utilisation des numéros AVS en dehors de l'assurance sociale de la Confédération n'est pas nécessaire pour la perception des redevances et n'est donc pas proportionnée du point de vue de la protection des données. Nous avons toujours proposé d'utiliser un numéro spécifique au domaine ou au secteur, ce qui réduirait considérablement la problématique de l'interconnexion entre les différentes bases de données. Des explications complémentaires sur ce thème figurent dans notre 21e rapport d'activités 2013/2014 au chiffre 1.2.8.

1.3.3 Nouveau service de bureautique au sein de l'administration fédérale (UCC)

Le programme «Unified Communication and Collaboration» (UCC) vise à remplacer le réseau téléphonique fixe par un nouveau standard de bureautique au sein de l'administration fédérale. Nous avons fait part aux responsables du projet de nos remarques sur les aspects de protection et de sécurité des données à prendre en compte. Nous suivons attentivement la mise en œuvre du programme.

Par décision du 9 novembre 2011 concernant la stratégie de la Confédération en matière de technologies de l'information et de la communication (TIC), le Conseil fédéral a chargé l'Unité de pilotage informatique de la Confédération (UPIC) d'élaborer le nouveau service standard de bureautique de l'administration fédérale, comprenant la communication vocale (téléphonie fixe et mobile), la visiophonie, la visioconférence, le partage d'écran, la messagerie instantanée, et la communication par courriel. L'intégration de ce service s'effectuera dans le cadre du programme UCC qui devrait se terminer d'ici à fin 2015.

La Chancellerie fédérale (ChF) a décidé d'introduire rapidement cette migration afin de pouvoir continuer à jouer au mieux son rôle de coordination entre les départements. Le Préposé fédéral à la protection des données et à la transparence (PFPDT) étant rattaché administrativement à la ChF, nous sommes dès lors concernés aussi bien en tant qu'utilisateurs que comme organe de conseil et de surveillance des organes fédéraux en matière de protection des données. C'est à ce titre que nous avons été invités à une présentation du projet dans le cadre d'une séance du groupe de travail interdépartemental (GTID) «Protection des données». La présentation a soulevé plusieurs questions, en particulier quant à la conformité des bases légales et quant à l'existence d'un concept de sûreté de l'information et de protection des données (SIPD) selon les exigences de la procédure HERMES. Les participants ont également été surpris d'avoir été informés respectivement consultés aussi tardivement sur ce sujet.

La première version du concept SIPD a ainsi été complétée à notre demande par un document contenant entre autres une description détaillée des risques résiduels et une analyse des bases légales sous l'angle de la protection des données et de la sécurité des informations. Les responsables du projet ont également effectué une analyse d'impact relative à la protection des données, en utilisant l'instrument mis à disposition sur notre site (https://www.apps.edoeb.admin.ch/dsfa/fr/index.html). Sur la base de ces nouveaux documents, nous avons pris position en soulignant les éléments à prendre en compte sous l'angle de la protection et de la sécurité des données:

Du point de vue technique, nous avons été étonnés d'apprendre que ce service ne permettrait – comme jusqu'à présent – que les communications téléphoniques de sensibilité «interne», alors que les protocoles cryptographiques mis en œuvre auraient théoriquement pu permettre une protection adéquate pour des conversations de niveau «confidentiel» ou «sensible». Nous avons en outre plaidé pour le maintien d'une confidentialité aussi élevée que jusqu'à présent et proposé d'effectuer une expertise neutre de risques. Nous avons relevé l'importance de garantir une disponibilité équivalente à l'ancienne solution (réseau physique séparé). Nous nous interrogeons au final sur la pertinence du choix du client MS-Lync 2013.

Du point de vue juridique, il ne nous a malheureusement pas été possible de nous prononcer définitivement, certains détails liés en particulier aux données secondaires et à leur enregistrement n'étant pas clairs. Nous avons cependant confirmé que malgré les incertitudes qui subsistaient, des bases légales supplémentaires ne paraissaient pas nécessaires. Nous avons relevé que ceci ne saurait être interprété comme une autorisation formelle pour l'introduction du système. La responsabilité d'un tel traitement incombe en effet à l'exploitant du service (donc chaque autorité), celle de sa mise en œuvre à l'UPIC. Nous espérons que l'UPIC tiendra compte de nos remarques et conseils.

Il va de soi que nous resterons vigilants au sujet de l'évolution de ce projet, au gré de nos expériences concrètes dans ce nouvel univers du couplage téléphonie-informatique et des éventuels problèmes constatés par les utilisateurs des autres offices fédéraux. Le cas échéant, nous ne manquerons pas d'intervenir auprès des instances concernées.

1.3.4 Accès gratuit au réseau WiFi des CFF

Depuis l'automne 2014, les CFF offrent un accès gratuit à Internet dans différentes gares («Free WiFi CFF»). Nous leur avons demandé quelles données ils traitaient et leur avons signalé qu'ils ne pouvaient, sur la base des conditions générales en vigueur, ni traiter les données des utilisateurs à des fins de marketing, ni analyser les flux de personnes.

En septembre 2013, les CFF ont activé un service de WiFi gratuit («Free WiFi CFF») dans différentes gares. Les clients qui souhaitent profiter de cette offre doivent s'enregistrer et confirmer qu'ils ont lu et accepté les conditions d'utilisation. Dans les conditions générales correspondantes, les CFF se réservent le droit de traiter les données à différentes fins, notamment pour analyser les déplacements des clients. Nous avons contacté les CFF afin de clarifier les faits. Le sujet a également été abordé lors d'une séance entre le CEO des CFF et le Préposé fédéral à la protection des données et à la transparence.

Nos clarifications ont montré d'une part que les CFF traitaient les données sur la seule base de la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT), et notamment que le traitement des données à des fins de marketing n'était pas encore mis en œuvre. D'autre part, nous avons constaté que les conditions d'utilisation étaient formulées de manière trop imprécise et ne détaillaient pas quelles données étaient utilisées à quelles fins. Par conséquent, le consentement requis pour un traitement à des fins de marketing et pour l'analyse de flux de personnes ne serait pas valable sur la base de ces conditions d'utilisation. Les conditions générales ont donc dû être adaptées en conséquence. En revanche, les CFF disposent d'une base légale, et donc d'un motif justificatif, pour un traitement de données personnelles fondé sur la LSCPT. Cependant, les conditions générales prévoient que les données seraient conservées douze mois au lieu des six mois actuellement prévus dans la loi. Elles ont donc dû être adaptées en conséquence.

Nous avons communiqué aux CFF les résultats de notre analyse. Les CFF n'ont à ce jour (31 mars 2015) pas encore modifié leurs conditions générales.

1.3.5 Stratégie Open Government Data de la Confédération

Nous avons pris position dans le cadre de la consultation des offices concernant la Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2014 à 2018. Nous avons explicité les exigences sous l'angle de la protection des données.

Les données publiques librement accessibles ne contiennent pas d'informations personnelles. Pourtant, il existe un risque que des informations personnelles soient mises en relation avec d'autres données. C'est pourquoi, dans notre prise de position répondant à la consultation des offices sur la Stratégie Open Government Data Suisse 2014 – 2018, nous rappelons l'importance de la prise en compte des aspects juridiques de la protection des données dès la phase de planification et de développement de projets en matière de données publiques librement accessibles. Nous avons suggéré que le document stratégique prévoie des procédures incluant des mesures techniques et organisationnelles afin de prévenir toute divulgation accidentelle de données personnelles. Si l'autorité s'appuie sur le fait que seuls des paquets de données agrégées et anonymes sont publiés, elle doit effectuer une estimation approfondie des incidences en matière de protection des données afin d'empêcher l'identification de personnes physiques ou morales.

1.3.6 Protection du droit d'auteur sur Internet

Les modifications du droit d'auteur proposées par AGUR 12 doivent être maintenant mises en œuvre dans la législation. Nous suivons le processus législatif et veillons au maintien de la protection de la personnalité.

En décembre 2013, le groupe de travail AGUR 12 institué par la Conseillère fédérale Simonetta Sommaruga a présenté son rapport final (cf. notre 21e rapport d'activités 2013/2014, ch. 1.3.1). Les modifications proposées doivent être maintenant vérifiées et mises en œuvre. Nous approuvons le fait que l'on ait éliminé l'insécurité du droit régnant actuellement au sujet de la collecte et le traitement de données personnelles en lien avec des violations du droit d'auteur sur Internet. En parallèle, nous entendons contribuer à ce que les mesures introduites tiennent compte de la protection de la personnalité. Nous suivons donc les développements en cours et accompagnerons le processus législatif.

1.3.7 Publication sur Internet de rapports sur des enseignants

La publication sur Internet de rapports concernant l'influence politique exercée par des enseignants peut porter atteinte aux droits de la personnalité des personnes concernées. Il convient donc de veiller à ce que de tels textes ne soient publiés que sous forme anonymisée.

L'endoctrinement politique dans le cadre de l'enseignement scolaire est un thème délicat. Les enseignants ne réussissent pas toujours à rester politiquement neutres en dispensant leurs cours. Lorsque des thèmes politiques ou sociaux sont abordés, les opinions politiques des enseignants sont susceptibles de parvenir jusqu'aux élèves, volontairement ou non. Fort de cette constatation, un parti politique vient de lancer un site Internet sur lequel il est possible de débattre publiquement de ce genre de faits. Cette action avait pour but de dissuader les enseignants de faire état trop librement de leur opinion politique devant leurs élèves afin de les influencer dans leur sens.

Ce type de plateforme est susceptible de porter atteinte aux droits de la personnalité des enseignants concernés. Comme dans le cas des mises au pilori sur Internet (cf. notre 20e rapport d'activités 2012/2013, ch. 1.3.1), les enseignants cités peuvent y être stigmatisés et inutilement dénigrés sans avoir la possibilité de se défendre. Dans ce cas, un motif justificatif ne paraît pas donné. La garantie d'un enseignement politiquement neutre peut certes être qualifié d'intérêt public, il n'appartient cependant pas à des particuliers d'assurer sa mise en œuvre. Il existe dans tous

les cantons des organes de surveillance auprès desquels les cas d'influence politique des enseignants peuvent être annoncés. Ces organes ont la compétence de prendre des mesures adaptées.

Du fait que le site en question a pour but la publication de «rapports» commentant l'influence politique exercée par certains enseignants et, de ce fait, thématise les opinions ou activités politiques des personnes en question, les données qui y sont traitées sont considérées comme des données sensibles par la loi sur la protection des données. De fait, nous avons reçu un très grand nombre de demandes à propos de ce site. Nous avons donc ouvert une procédure d'établissement des faits. Il est apparu que tous les commentaires postés avaient été contrôlés et anonymisés de sorte que le lecteur ne peut en général détecter de quel enseignant il s'agit. Le site en question ne peut donc pas être considéré dans sa forme actuelle comme un site de mise au pilori sur Internet.

Il convient toutefois de souligner qu'il ne suffit pas de supprimer les noms pour anonymiser un texte. Effectivement, la situation ou les circonstances décrites peuvent aisément permettre de reconnaître les enseignants mentionnés. Pour cette raison, l'anonymisation de ce type de rapports doit être faite avec beaucoup de précaution et si cela n'est pas possible, il convient de renoncer à la publication.

1.4 Justice/Police/Sécurité

1.4.1 Protection des données dans le cadre de la deuxième évaluation Schengen

Lors de la deuxième visite d'évaluation Schengen en Suisse, ce sont les compétences du préposé fédéral, d'autres organes fédéraux et de plusieurs autorités cantonales de protection des données qui ont été examinées. Cette deuxième évaluation s'est conclue par un bilan positif.

L'acquis de Schengen est en constante évolution. La mise en œuvre et l'application correcte des dispositions Schengen sont soumises à un contrôle régulier, environ tous les quatre ans, dans tous les États Schengen.

La première évaluation de la Suisse a eu lieu en 2008 et a permis la mise en fonction du système d'information Schengen (SIS). La deuxième évaluation a eu lieu au printemps 2014: entre mars et juillet, cinq équipes composées d'experts du Conseil européen, de la Commission européenne et des autres États Schengen ont procédé à la deuxième évaluation Schengen. Celle-ci portait sur l'application correcte des dispositions Schengen relatives à la coopération policière, à la protection des données, aux visas, à la protection des frontières extérieures et au Système d'information Schengen de deuxième génération (SIS II).

L'évaluation de protection des données portait sur l'implémentation de l'Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne, sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (AAS), en particulier sur les compétences de l'autorité de contrôle fédérale (PFPDT) et des autorités cantonales de protection des données. Celles-ci ont été évaluées sur la base d'un questionnaire et d'inspections locales. Les compétences de surveillance, d'investigation et d'intervention des autorités de contrôle ainsi que l'indépendance de ces dernières ont été en particulier examinées. Ce sont les bases légales et spécialement les compétences de contrôle sur le SIS II et les services impliqués dans sa gestion qui ont été analysées. Les droits des personnes concernées, la sécurité des données, la coopération avec les autorités étrangères et l'information du public ont également été soumis à évaluation.

Nous nous sommes fortement investis dans le cadre de la préparation de cette évaluation, en étroite collaboration notamment avec l'Office fédéral de la Justice (OFJ), l'Office fédéral de la Police (fedpol), le Secrétariat d'État aux migrations (SEM), le Département fédéral des affaires étrangères (DFAE) et les autorités cantonales de protection des données. Il s'agissait de répondre au questionnaire d'évaluation

adressé à la Suisse par l'Union européenne (juin 2013) et de se préparer en vue des inspections locales. La visite d'évaluation en matière de protection des données auprès des autorités suisses a eu lieu du 12 au 16 mai 2014. Le groupe d'experts a inspecté les compétences du PFPDT et des autorités de protection des données des cantons de Neuchâtel/Jura et du canton de Berne qui figuraient au programme de la visite.

L'évaluation a fait l'objet d'un rapport relatif à la protection des données. En date du 18 novembre 2014, le Conseil de l'UE au niveau ministériel a formellement mis un terme à la deuxième évaluation Schengen en constatant que, globalement, les exigences en matière de protection des données découlant de l'Accord d'Association à Schengen étaient remplies en Suisse – La prochaine évaluation de la Suisse est prévue pour 2018.

1.4.2 Projet de loi sur le renseignement

Le projet de loi sur le renseignement a été transmis au Parlement. Nous avons défendu notre position lors d'une audition de la Commission de la politique de sécurité du Conseil national.

Nous avons été auditionnés par la Commission de la politique de sécurité du Conseil national afin de pouvoir faire part de notre position concernant le projet de loi sur le renseignement: nous avons dans ce cadre salué les différents contrôles prévus pour les mesures d'acquisition des informations soumises à autorisation et les mesures de sécurité des données (traitement des données dans un fichier spécifique accessible à un nombre restreint de collaborateurs). Afin de garantir une surveillance efficace dans ce domaine, nous avons proposé que l'organe de surveillance interne du département et la Délégation des commissions de gestion soient tenues de contrôler systématiquement toutes les mesures d'acquisition soumises à autorisation. Nous avons également soutenu qu'il conviendrait de veiller à garantir également un contrôle externe indépendant des traitements de données afin de vérifier et de s'assurer que le cadre légal a été respecté et que les mesures ordonnées étaient adéquates et vraiment nécessaires.

Nous avons indiqué une nouvelle fois (cf. notre 21e rapport d'activités 2013/2014, ch. 1.4.6 et ch. 2.5.1) que ce projet contient encore un certain nombre d'éléments problématiques du point de vue de la protection des données: l'utilisation d'aéronefs et de satellites, la possibilité de s'introduire dans des systèmes et des réseaux informatiques ainsi que l'exclusion de la «collecte d'informations selon la loi sur le renseignement» du champ d'application de la loi sur la transparence. Lors de cette audition, nous avons également rappelé que l'exploration du réseau câblé, malgré les règles proposées, engendrerait des risques élevés d'atteinte à la personnalité.

1.4.3 Révision de l'ordonnance sur les systèmes d'information du SRC

Nous avons pris position sur la révision de l'ordonnance sur les systèmes d'information du Service des renseignements de la Confédération. Nos remarques concernant la règlementation prévue pour les contrôles périodiques effectués dans le système d'information pour la sécurité extérieure ISAS et dans les autres systèmes d'informations du Service de renseignement de la Confédération ont été prises en compte.

La modification du 21 mars 2014 de la loi fédérale sur le renseignement civil (LFRC) et l'ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC) sont entrées en vigueur le 1er novembre 2014. Depuis cette date, le système d'information pour la sécurité extérieure (ISAS) ne constitue plus un essai pilote mais un fichier disposant d'une base légale définitive. En plus des adaptations rendues nécessaires par la révision de la LFRC, l'ordonnance OSI-SRC a été entièrement restructurée afin d'en améliorer la clarté.

Dans le cadre de la consultation des offices, nous avons estimé que les solutions proposées concernant les différents contrôles périodiques dans ISAS et dans les autres systèmes d'information du Service de renseignement de la Confédération (SRC) n'étaient pas satisfaisantes (par contre, les contrôles relatifs au système d'information pour la sécurité intérieure (ISIS) n'ont pas fait l'objet de remarques de notre part). Après plusieurs discussions avec le SRC, des solutions ont pu être trouvées:

Les collaborateurs du SRC chargés de saisir les données contrôlent périodiquement les blocs de données contenues dans ISAS qui comportent des objets relatifs à des personnes ou à des organisations. Ils apprécient au vu de la situation actuelle si les blocs de données sont encore utiles à l'accomplissement des tâches assignées au SRC. Ils effacent les données dont le SRC n'a plus besoin. Ils rectifient, marquent ou effacent les données qui s'avèrent inexactes. Enfin, ils consignent l'exécution et le résultat du contrôle. Le contrôle périodique a lieu chaque fois qu'un bloc de données est complété. Dans tous les cas, un contrôle périodique est effectué, en fonction des domaines, dix à vingt ans après la saisie de l'objet ou le dernier contrôle périodique. De plus, le service chargé d'assurer la qualité procède à des contrôles qu'il effectue au moins une fois par an selon un plan de contrôle.

Le service chargé d'assurer la qualité contrôle par sondage la légalité du traitement des données saisies dans les autres systèmes d'information du SRC, son adéquation, son efficacité et son exactitude. Il effectue ce contrôle au moins une fois par an pour chaque système d'information selon un plan de contrôle.

1.4.4 Révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

Durant l'année sous revue, nous avons participé aux séances de la Commission des affaires juridiques du Conseil national concernant la révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. La question de la publication de données dites secondaires obtenues au cours d'une surveillance rétroactive a également été abordée.

L'année dernière, la Commission des affaires juridiques du Conseil national nous a invités aux séances consacrées au projet de révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). À cette occasion, nous avons rappelé notre position déjà exprimée à l'occasion de la consultation des offices, à savoir que l'atteinte à un droit fondamental garanti par la Constitution nécessite des bases légales formelles et matérielles qui doivent être formulées avec suffisamment de précision. Nous avons également souligné que la conservation de données doit demeurer proportionnée d'un point de vue temporel par rapport à la finalité poursuivie (cf. notre 20e rapport d'activités 2012/2013, ch. 1.4.5 et notre 19e rapport d'activités 2011/2012, ch. 1.4.8).

Si la LSCPT révisée est adoptée par les Chambres, nous suivrons les révisions totales des ordonnances et serons particulièrement attentifs au respect du cadre prévu par la loi.

1.4.5 Révision de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (JANUS)

L'utilisation d'outils informatiques impliquant des traitements de données sensibles ou des profils de la personnalité dans le cadre des systèmes d'information de la Police judiciaire fédérale doit reposer sur une base légale au sens formel. Nous l'avons indiqué dans le cadre de la consultation des offices concernant la révision de l'ordonnance sur le système informatisé de la Police judiciaire fédérale JANUS.

L'Office fédéral de la police (fedpol) a développé des instruments informatiques pour rendre plus efficaces les traitements d'informations destinées au système d'appui aux enquêtes de police judiciaire de la Confédération, au système de traitement des données relatives aux infractions fédérales et au système de traitement des données relatives à la coopération policière internationale et intercantonale. Afin de permettre une exploitation de ces instruments informatiques de manière conforme au droit, fedpol a proposé une révision de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (ordonnance JANUS).

Dans le cadre de la consultation des offices, nous avons fait remarquer que l'utilisation de ces outils informatiques n'était pas expressément prévue par la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) et que les modifications de l'ordonnance JANUS soulevaient ainsi des problèmes de légalité, les dispositions prévues ne se fondant pas sur une base légale suffisante (en particulier les dispositions concernant les fonctionnalités de ces outils informatiques dans lesquels des données sensibles sont conservées). Comme il s'agit uniquement d'outils informatiques pour faciliter le traitement de données destinées aux systèmes d'information susmentionnés, une réglementation a été prévue de manière temporaire au niveau de l'ordonnance. Lors de la prochaine révision de la LSIP, ces outils informatiques seront expressément mentionnés dans une base légale au sens formel.

1.4.6 Modification des bases légales liées au développement de l'armée

Conformément à nos remarques, des précisions et explications concernant l'exigence des analyses de sang ou des vaccinations à titre préventif et celle des examens médicaux de routine ont été apportées dans le message au Conseil fédéral. De même, notre demande de limiter les examens médicaux de routine à un nombre restreint de personnes a été suivie. En revanche, notre position selon laquelle l'assujettissement de militaires à des contrôles de sécurité sans leur consentement est, sauf exception, contraire au principe de proportionnalité a fait l'objet d'une divergence dans la proposition au Conseil fédéral.

Dans le cadre des différentes consultations des offices relatives à la modification des bases légales liées au développement de l'armée, nous avons formulé plusieurs remarques.

Le projet de modification de la loi fédérale sur l'armée et l'administration militaire (LAAM) prévoit que le Conseil fédéral peut, pour l'exercice de fonctions de l'armée présentant un risque élevé d'infection, exiger des analyses de sang ou des vaccinations à titre préventif. Nous avons demandé que le message relatif au projet de loi soit beaucoup plus précis quant aux différentes analyses de sang et aux différents vaccins prévus ainsi qu'aux fonctions nécessitant de telles mesures. L'indication, à titre d'exemple, du personnel sanitaire ou de personnes engagées à l'étranger était trop vague. Il est de notre avis nécessaire que le message définisse des limites dans lesquelles le Conseil fédéral pourra concrétiser dans l'ordonnance d'application les mesures mentionnées dans la loi. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a tenu compte de nos remarques et a modifié le message dans le sens des considérations mentionnées ci-dessus.

D'autre part, le projet de modification de la LAAM stipulait dans un premier temps que le DDPS peut prévoir, pour le personnel militaire et les cadres du rang le plus élevé de l'administration militaire de la Confédération, des examens médicaux de routine réguliers, effectués par un médecin de confiance ou par le service médical. A l'heure actuelle, de tels examens médicaux de routine sont facultatifs et ne concernent qu'un nombre restreint de personnes (officiers d'état-major de haut rang et cadres du rang le plus élevé de l'administration militaire de la Confédération). Le projet proposait d'élargir de manière importante le cercle des personnes touchées (personnel militaire et cadres du rang le plus élevé de l'administration militaire de la Confédération) mais en plus de rendre ces examens médicaux de routine obligatoires. Les indications succinctes figurant dans le message ne permettaient pas de vérifier si une telle mesure respectait le principe de proportionnalité. Il apparaissait aussi étonnant que l'ensemble du personnel militaire doive être soumis à des examens médicaux de routine. Nous avons donc demandé de réduire le cercle des personnes concernées par de tels examens. Le DDPS a tenu compte de nos remarques et les examens médicaux de routine concerneront les officiers généraux, le personnel militaire de la police militaire et les cadres du rang le plus élevé de l'administration militaire de la Confédération.

Le projet de modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) quant à lui prévoit que les militaires peuvent être assujettis au contrôle de sécurité même sans leur consentement si cette formalité est requise pour l'exercice de la fonction militaire actuelle ou prévue. Les militaires pouvant se voir attribuer une fonction contre leur gré, nous sommes d'avis que la possibilité de mener de tels contrôles de sécurité sans le consentement des personnes concernées ne respecte pas le principe de proportionnalité. De plus, nous estimons qu'attribuer une fonction à une personne contre son gré est problématique du point de vue de la sécurité. Nous pouvons cependant admettre que dans des cas exceptionnels, un contrôle de sécurité sans le consentement de la personne concernée puisse être justifié. Le DDPS dans ce cas n'a pas tenu compte de nos remarques. Cette divergence a été mentionnée dans la proposition au Conseil fédéral.

1.4.7 Contrôle des logfiles auprès du Secrétariat d'État aux migrations en tant qu'utilisateur final du SIS

Dans le cadre des accords d'association à Schengen, nous avons procédé à un contrôle des logfiles auprès du Secrétariat d'État aux migrations (SEM) en tant qu'utilisateur final du Système d'information Schengen (SIS). L'analyse des logfiles a montré que l'accès au SIS par les sections régionales du SEM était conforme.

Dans le cadre des accords d'association à Schengen, nous effectuons annuellement des contrôles auprès des utilisateurs finaux du SIS. Nous nous sommes concentrés cette année sur les sections régionales du Secrétariat d'État aux migrations (SEM, anciennement Office fédéral des migrations/ODM), dont les principales tâches sont de traiter les cas individuels en matière de visa, d'approuver les autorisations de séjours ainsi que de traiter les mesures d'éloignement. Pour toute la durée du contrôle, le conseiller à la protection des données du SEM a été notre principal partenaire de discussion.

Pour ce contrôle, nous avons sélectionné de manière aléatoire trois sections régionales du SEM. Après avoir annoncé le contrôle au SEM, nous avons reçu la liste des collaborateurs des trois sections concernées puis immédiatement contacté l'Office fédéral de la police (fedpol) pour recevoir les logfiles qui listent les accès au SIS de ces collaborateurs durant la semaine choisie.

Le contrôle a été annoncé au SEM mais les collaborateurs concernés n'avaient pas été informés que leurs accès au système allaient être analysés.

Nous avons procédé à l'analyse dans nos locaux sur la base des documents fournis par fedpol. Notre examen portait principalement sur le nombre d'accès par section et par collaborateur ainsi que sur le contenu des recherches effectuées.

Nous avons ainsi pu constater que les pratiques mises en place par les trois sections différaient, en particulier les collaborateurs principalement en charge des recherches dans le système n'occupaient pas les mêmes fonctions. Toutefois, aucun abus n'a été constaté. De plus, aucune recherche n'a semblé suspecte ou inappropriée. L'analyse des logfiles a montré que l'accès au SIS par les sections régionales du SEM était conforme. Nous avons donc clos le contrôle sans avoir à effectuer de visite sur place.

1.5 Santé et recherche

1.5.1 Remise du dossier médical original

Un patient peut, sur la base de la loi fédérale sur la protection des données, exiger de son médecin qu'il lui remette une copie de son dossier médical complet. La loi sur la protection des données ne fonde cependant pas un droit à la remise de l'original.

Pendant l'année sous revue, nous nous sommes à nouveau intéressés au débat juridique concernant la remise de l'original du dossier médical par un médecin. Ce sujet a été soulevé par la demande d'un psychiatre du canton de Zurich, auquel un patient demandait l'original de son dossier médical en invoquant le droit d'accès au sens de l'article 8 de la loi fédérale sur la protection des données (LPD). Le psychiatre a alors contacté le service du médecin cantonal de Zurich pour savoir s'il pouvait remettre l'original des documents en question au patient. On lui a répondu que la disposition applicable de la loi sur la santé du canton de Zurich constitue du droit public impératif et qu'elle impose aux professionnels de la santé la conservation des documents originaux pendant une durée de dix ans.

Le psychiatre nous a fait parvenir cette prise de position afin de connaître notre avis. Après un échange d'informations avec le service du médecin cantonal, nous avons constaté que les dispositions déterminantes du canton de Zurich obligeaient effectivement les professionnels de la santé à conserver les originaux des documents relatifs aux traitements pendant une période de dix ans. Étant donné la nature impérative de cette disposition de droit public, nous sommes parvenus à la conclusion que le professionnel de la santé ne peut être libéré de cette obligation de conservation par un accord individuel convenu avec le patient. Il est donc exclu de remettre l'original du dossier médical dans le canton de Zurich pendant la durée de conservation légale.

Les discussions nous ont amenés à formuler notre position sur ce point. Nous constatons concrètement qu'un droit à la remise du dossier médical sous sa forme originale ne peut être déduit du seul droit d'accès au sens de l'art. 8 LPD. Les renseignements doivent généralement être fournis par écrit, sous forme de copies ou d'un imprimé. Il ne nous appartient pas de juger de l'existence éventuelle d'un droit à la remise de l'original du dossier médical découlant du droit des mandats, ou de son applicabilité dans le canton concerné. Une consultation sur place est possible, mais uniquement si le patient y consent. Si le médecin craint un «éclaircissement dommageable», il est autorisé à transmettre l'imprimé ou la copie du dossier médical à un médecin désigné par le patient, qui pourra l'assister pour prendre connaissance du dossier et le préserver d'un éventuel préjudice.

Cette procédure représente selon nous un cas exceptionnel car les patients devraient être généralement bien informés de leur état de santé pendant un traitement, du fait des obligations d'information incombant au médecin, et peuvent se renseigner de manière relativement rapide et aisée sur la signification de termes techniques. La copie du dossier médical doit en principe être remise gratuitement au patient. Le médecin ne peut demander une participation aux frais, à hauteur de 300 francs au maximum, que pour autant que la remise de la copie entraîne des coûts particulièrement élevés ou que le patient a déjà demandé une copie dans les douze derniers mois.

1.5.2 Vente forcée de données de patients dans le cadre d'une procédure de faillite

Un office des faillites ne peut vendre des données de patients à un successeur prêt à racheter le cabinet sans avoir préalablement consulté les patients. L'accord des patients constitue une condition indispensable à la transmission des données à l'acquéreur du cabinet.

Le fait que les données des patients possèdent une valeur marchande a été confirmé par un office des faillites pendant l'année sous revue. L'office cantonal envisageait la vente forcée du fichier de patients d'un dentiste avec les dossiers médicaux, sans en informer les patients concernés au préalable. Il nous a contactés afin d'obtenir notre avis sur la faisabilité d'un tel projet, tout en sachant que nous ne sommes en réalité pas compétents puisque l'office des faillites est un organe cantonal soumis à la surveillance du préposé cantonal à la protection des données. Nous avons dû informer l'office des poursuites qu'il ne pouvait procéder à la vente forcée du fichier de patients et des dossiers s'y rapportant sans consulter préalablement les personnes concernées.

Conformément à la loi fédérale sur la protection des données (LPD), un consentement n'est valable que si la personne exprime sa volonté librement et après avoir été dûment informée. Les données des patients constituant des données sensibles au sens de la LPD, le consentement doit au surplus être explicite (art. 4, al. 5 LPD). Par ailleurs, il est à noter que le dentiste est ici soumis à une obligation cantonale de conservation qui reste valable au-delà de l'exploitation du cabinet.

1.5.3 Vol de données de patients dans un cabinet médical

Si un ordinateur contenant des données de patients est volé dans un cabinet, le médecin concerné n'est pas soumis à un devoir légal d'en informer le PFPDT. Il peut toutefois être judicieux d'informer les patients.

Le vol d'un ordinateur personnel est une expérience pénible. Les photos souvenirs ou les courriers importants sont perdus pour toujours si aucune sauvegarde n'a été réalisée. Mais cela est particulièrement sensible lorsqu'un ordinateur contenant des données de patients est volé dans un cabinet médical.

Un médecin concerné par un tel vol nous a contactés par téléphone afin de savoir s'il devait informer ses patients ou une autorité de surveillance. Contrairement à la situation prévalant dans certains pays européens, le droit suisse ne prévoit pas une telle procédure en cas de perte ou de communication frauduleuse à des tiers de données sensibles. Le principe de transparence découlant du droit de la protection des données pourrait néanmoins aboutir à une obligation d'information des personnes concernées, puisqu'un pareil cas génère une communication de données certes involontaire, mais non compatible avec la finalité initialement prévue. Quoi qu'il en soit, l'information des patients peut être jugée pertinente pour une autre raison. Si les patients prenaient connaissance du vol par un autre moyen, la relation de confiance avec leur médecin en serait affectée.

Du point de vue du droit de la protection des données, il convient également de noter que le médecin doit prendre des mesures techniques appropriées pour protéger les données de ses patients d'accès non autorisés. Les mesures en question doivent correspondre à l'état actuel de la technique et être adaptées au caractère sensible des informations. La simple protection par identifiant et mot de passe ne suffit pas pour les informations médicales: il convient en effet de faire appel à des technologies de cryptage adaptées. Il est certain que la doctoresse en question aurait été plus sereine face à ce vol si les données stockées sur son ordinateur avaient été cryptées.

1.5.4 Établissement des faits auprès du service médical de la Confédération (MedicalService AeD)

Durant l'année sous revue, nous avons engagé une procédure d'établissement des faits auprès du service médical de la Confédération et des entreprises fédérales (Medical Service AeD). Nous avons examiné en particulier le traitement des données sur la santé de candidats effectué dans le cadre d'une postulation.

Suite à un nombre relativement important de demandes de citoyens, nous avons – dans le cadre de notre activité de surveillance – engagé en automne 2014 une procédure d'établissement des faits auprès du service médical de la Confédération et des entreprises fédérales – MedicalService AeD – concernant les données de santé dans le domaine du travail. Nous évaluons actuellement si le traitement des données concernant la santé de candidats répond aux exigences en matière de

protection des données. Notre examen porte principalement sur le traitement des données effectué par MedicalService AeD, ainsi que sur le flux de données entre le service médical et l'employeur.

L'Office fédéral du personnel ayant délégué sa compétence à MedicalService AeD, ce dernier est soumis à la loi fédérale sur le personnel de la Confédération qui l'autorise dans certains cas à traiter des données personnelles sensibles sur la santé. Selon la loi, le service médical ne peut informer les services intéressés que des «conclusions des constats médicaux». Il peut donc indiquer par exemple si le candidat a ou non le profil pour le poste au vu de sa santé. En revanche, il ne peut en aucun cas communiquer un diagnostic proprement dit à des tiers sans l'accord écrit de la personne concernée. Nous estimons nécessaire, dans le cadre d'une procédure d'établissement des faits, d'étudier plus en profondeur les traitements de données effectués dans ce domaine et d'en évaluer la conformité avec la loi fédérale sur la protection des données (LPD).

La première partie de la procédure est close. Les faits ont été établis sur la base de l'ensemble des documents reçus. Dans une prochaine étape, nous effectuerons une visite auprès de MedicalService AeD, afin d'examiner de manière plus détaillée si les processus et les traitements de données satisfont aux exigences de la LPD.

1.5.5 Conservation de dossiers médicaux dans le nuage

De plus en plus de médecins désirent conserver le dossier de leurs patients dans un nuage informatique. Si cette méthode offre maints avantages, elle n'en est pas moins problématique en raison de la protection du secret médical en droit pénal. En cas d'externalisation de la conservation des dossiers, il s'agit surtout d'assurer que des tiers ne puissent traiter indûment les données des patients.

La loi sur la protection des données autorise la transmission à un tiers du traitement de données personnelles et, de ce fait, la gestion de dossiers médicaux. Cela néanmoins uniquement à la condition que les données en question ne soient traitées que comme le mandant (en l'occurrence le médecin) serait en droit de le faire lui-même et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise. En vertu du droit pénal, les médecins sont tenus au secret professionnel pour ce qui concerne les antécédents médicaux ou le contenu du dossier médical. Il s'agit d'une obligation légale de garder le secret qui ne peut être déléguée à un tiers, ou uniquement sur la base d'un contrat. La responsabilité du traitement des données de patients demeure ainsi auprès du médecin.

Nous avons enjoint tous les médecins et fournisseurs de services informatiques en nuage qui se sont adressés à nous de se reporter à nos explications concernant

l'informatique en nuage (cloud computing) afin de les sensibiliser à cette thématique. Nous avons attiré en particulier leur attention sur ceci: lorsqu'un médecin délègue le traitement des dossiers de ses patients à un tiers, il demeure responsable du respect du secret médical. Il devrait donc veiller à ce que la sécurité des données auprès de tiers, donc dans le nuage (réseau dématérialisé) soit garantie conformément à la loi sur la protection de données. En d'autres termes, les données des patients doivent être protégées par des mesures techniques et organisationnelles adéquates contre tout traitement indu. Le médecin doit contrôler et surveiller la confidentialité, la disponibilité et l'intégrité des données.

Pour cette raison, pour un médecin exerçant en Suisse, il n'y a selon nous que la solution suivante: le fournisseur de services informatiques en nuage et le nuage doivent être en Suisse et garantir de manière contractuelle au médecin que les données des patients ne quittent pas la Suisse. Les données des patients doivent être systématiquement chiffrées de sorte que le médecin en qualité de maître du fichier soit la seule personne à posséder la clé permettant d'accéder aux données se trouvant dans le nuage. Le fournisseur de services en nuage ne doit pas avoir accès à cette clé. Le maître de fichier, soit le médecin, peut transmettre les données à des fins statistiques, mais il doit les avoir totalement anonymisées auparavant. À notre avis, ces mesures sont les seules à garantir totalement que le médecin est à même de respecter le secret médical auquel il est tenu en vertu du droit pénal et qu'à aucun moment, les données des patients ne sont traitées de manière injustifiée.

1.5.6 Cybersanté – Identification des patients et accès aux dossiers électroniques

Le projet Cybersanté entre dans une phase décisive. Après l'approbation des recommandations V, des spécifications détaillées sont en cours de définition au sujet de l'identification des patients et des droits d'accès au dossier électronique des patients. Ces spécifications constituent la base de la mise en œuvre proprement dite du projet, mais aussi de l'ordonnance relative à la loi fédérale sur le dossier électronique du patient (LDEIP).

Afin que les mesures de protection des données que nous avons obtenues ne soient pas sacrifiées au cours de la mise en œuvre du projet, nous avons décidé de continuer à consacrer une petite partie de nos ressources limitées à la cybersanté (eHealth). Ce projet se trouve actuellement en phase de définition des procédures détaillées concernant le traitement du dossier électronique du patient. L'expérience a souvent montré que dans beaucoup de grands projets, à ce stade, la grande motivation existant à l'origine visant à promouvoir des solutions conformes à la protection des données, est tout simplement balayée. Les coûts et la complexité

sont alors invoqués comme arguments afin d'optimiser les systèmes et négliger les droits de la personnalité. Le projet de cybersanté n'est pas épargné par ce risque.

Grâce à des rectifications mineures mais permanentes, nous avons donc veillé et veillons encore à ce que dans les projets partiels, le droit de la protection des données ne reste pas seulement un but politique, mais soit aussi réellement mis en œuvre. Cela vaut tout particulièrement pour le mandat de l'organe de coordination Cybersanté pour les «spécifications de détails sur les droits d'accès», pour l'ordonnance relative à la LDEIP et pour la certification des communautés.

Nous avons défendu avec succès notre point de vue devant la Commission de la sécurité sociale et de la santé publique et plaidé en faveur de l'introduction d'un identifiant du patient indépendant du numéro AVS. La commission tout comme le Conseil des États ont suivi notre argumentation et approuvé le projet du Conseil fédéral.

1.5.7 Projet de loi fédérale sur l'enregistrement des maladies oncologiques

Le Conseil fédéral a soumis au Parlement le projet de loi visant à recenser les cas de cancer en Suisse. Lors de la deuxième consultation des offices, nous avons fait part de nos divergences pour la collecte de données supplémentaires et de nos réticences quant à l'utilisation du numéro AVS même pseudonymisé.

La Suisse va se doter d'un registre national des maladies oncologiques. Le Conseil fédéral a soumis son projet de loi au Parlement. Pour que la banque de données soit exhaustive, médecins, hôpitaux et autres institutions seront tenus d'annoncer les cas. Mais les patients pourront s'opposer en tout temps à l'enregistrement des données. La nouvelle loi règle la collecte, l'enregistrement et le transfert des données afin de pouvoir évaluer les informations contenues dans les registres des tumeurs cantonaux et les publier au niveau national. Il sera ainsi possible d'améliorer la prévention et la détection précoce ainsi que d'évaluer la qualité des soins, des diagnostics et des traitements.

Le gouvernement a revu son projet à l'aune des critiques émises lors de la procédure de la consultation. Il s'agissait en particulier de remarques sur les données collectées, leur protection et les droits des patients. La nouvelle version comporte certaines adaptations qui apportent des répercussions notables sur les droits des patients et comportent des risques d'atteintes aux droits fondamentaux des personnes concernées (voir nos précédentes remarques à ce sujet dans notre 21e rapport d'activité 2013/2014, chiffre 1.5.3).

Nous avons pris note que le Conseil fédéral a décidé de maintenir, malgré notre divergence à ce sujet, le numéro AVS comme identificateur de personnes dans les registres. Dans nos précédentes prises de position, nous avions attiré l'attention sur le fait que l'utilisation systématique du numéro AVS en tant qu'identifiant unique présente de gros risques pour la sphère privée des personnes concernées, en raison des connexions indésirables que cette extension permet d'établir entre différentes bases de données.

Nous avions ainsi préconisé l'introduction d'alternatives à l'utilisation du numéro AVS (par exemple identifiant sectoriel spécifique aux registres des cancers) en s'inspirant des développements concernant le numéro sectoriel d'identification des patients dans le cadre du projet de la loi fédérale sur le dossier électronique du patient (LDEIP). Cette approche a pour avantage de réduire le risque que les informations soient mises en relation, d'autant plus que les données du registre des tumeurs sont sensibles et permettent l'établissement de profils de la personnalité.

De plus, nous nous sommes exprimés en faveur du maintien du consentement explicite pour la collecte de données supplémentaires en lieu et place du droit d'opposition finalement retenu dans la nouvelle version, au motif qu'il s'agit de données sensibles permettant de mesurer l'évolution de la maladie, le déroulement du traitement, de même que de déterminer le milieu de vie des personnes concernées. Celles-ci peuvent être couplées avec les données de base et permettent ainsi d'obtenir des informations très détaillées sur l'état de santé d'une personne. L'exigence d'un consentement explicite est non seulement prévue à l'art. 4 al. 5 LPD mais également dans plusieurs lois récentes qui touchent aux droits de la personnalité des personnes concernées, telles la loi fédérale sur l'analyse génétique humaine (LAGH), la loi fédérale sur la procréation médicalement assistée (LPMA), la loi fédérale relative à la recherche sur l'être humain (LRH), de même que la loi fédérale relative à la recherche sur les cellules souches embryonnaires (LRCS).

Enfin, nous avons soutenu la solution d'une comparaison de la date du décès des registres des tumeurs aux fins d'actualisation et de complétude, non pas avec celle de la Centrale de compensation comme prévu dans le projet, mais avec celle des registres des habitants cantonaux ou d'état civil. En effet, la Centrale de compensation n'est pas un registre national des habitants et n'a pas la vocation de fournir à des autorités ou à des tiers des données de citoyens qu'elle traite à des fins d'assurances sociales.

1.6 Assurances

1.6.1 Contrôle des services de réception des données auprès des assureurs-maladie

Tous les assureurs-maladie doivent désormais disposer d'un service certifié pour la réception des factures de type DRG (forfaits par cas liés au diagnostic). Les contrôles que nous avons effectués auprès de douze services de réception des données ont montré que ces derniers fonctionnaient en général bien. Nous avons constaté toutefois quelques lacunes dans un petit nombre de cas que nous avons signalés aux services de certification concernés.

Durant l'année sous revue, nous avons examiné les services de réception des données de douze assureurs-maladies dans le cadre de mesures d'établissement des faits. Nous avons également évalué les interfaces entre hôpitaux, éventuels intermédiaires et services de réception de données ainsi qu'entre services de réception et assureurs.

Ces contrôles nous ont permis de constater ce qui suit:

La structure ou la forme des services de réception des données diffèrent fortement selon les assurances-maladie. Les grandes assurances sont nombreuses à avoir, dans leurs locaux, leur propre service de réception des données qui traite celles-ci sur la base de leurs propres systèmes, de systèmes achetés ou de systèmes sous licence. Les assurances de moyenne ou petite taille par contre ont tendance à externaliser le service de réception des données auprès d'un tiers qui agit pour leur compte. La transmission de données des hôpitaux au service de réception a toujours lieu par un intermédiaire. Certains services de réception sont très complexes et sont constitués de plusieurs systèmes de vérification combinés entre eux, d'autres encore ne comportent qu'un seul système.

La majeure partie des factures de type DRG sont transmises sous forme électronique. Cela montre qu'aujourd'hui, la plupart des prestataires sont équipés de manière à pouvoir livrer des factures électroniques. Malgré cela, nous avons constaté dans certains cas des différences étonnantes et difficilement compréhensibles entre les assureurs-maladie que nous avons contrôlés au sujet de la part des factures électroniques et des factures sur papier. Bien qu'il s'agisse souvent du même prestataire, les assureurs font l'objet de traitements différents. Ainsi, un assureur reçoit essentiellement des factures sur papier alors qu'un autre ne reçoit que des factures électroniques. Mais d'une manière générale, nous avons constaté qu'une majorité de prestataires n'établissaient que des factures électroniques.

Par ailleurs, nous avons observé que certains déduisaient de l'art. 59a de l'ordonnance sur l'assurance-maladie (OAMal) qu'il ne faudrait transmettre que les données

médicales au service de réception. Nous avons donc attiré l'attention de tous les acteurs concernés sur la formulation claire de la disposition, à savoir que toutes les données doivent être livrées au service de réception. C'est la seule manière de garantir que ce dernier puisse remplir sa fonction conformément à la loi, qui est de déterminer quelle facture nécessite un examen plus approfondi et d'assurer que seules les données dont l'assureur-maladie a vraiment besoin lui soient transmises (principe de la proportionnalité). Nous avons en outre souligné que les données administratives comportaient aussi des indications médicales, notamment le code DRG qui, dans la plupart des cas, donne une image claire de la santé du patient et de fait constitue une donnée médicale.

Dans le cadre des contrôles, nous avons en outre constaté qu'il n'est pas toujours clair de savoir quelles procédures de traitement relèvent du service de réception et sont de ce fait soumises à certification. Nous avons précisé aux assureurs-maladie, à leurs prestataires et à l'organisme de certification quels processus ou traitements de données doivent obligatoirement être effectués par le service de réception et dans quel ordre ces processus doivent avoir lieu. Tous les processus de vérification, qu'ils soient électroniques ou menés par des personnes qui décident si une facture doit être examinée de manière plus approfondie ou non, doivent être accomplis par le service de réception, indépendamment du fait qu'il s'agisse de processus concernant des factures sous forme papier ou sous forme électronique. En dehors du service de réception, aucune vérification systématique de toutes les factures ne doit avoir lieu. Tous les processus ou procédures de traitement de données relèvent du service de réception des données et doivent être certifiés.

A cet égard, surtout dans le cas des petites assurances-maladie, le problème suivant s'est parfois posé: les contrôles, qui servent à décider si un examen approfondi de la facture en question doit avoir lieu, sont effectués par des collaborateurs de l'assureur. Les fonctions de ces collaborateurs, font également partie du service de réception et doivent être certifiées. Cela peut poser des problèmes d'organisation au sein des petites assurances-maladie. Leurs employés occupent souvent une double fonction. D'une part, ils font partie du service de réception des données parce qu'ils effectuent les contrôles mentionnés plus haut, et d'autre part ils font partie du service des prestations et dans cette fonction, ils procèdent à l'examen plus approfondi des factures qu'ils se sont eux-mêmes adressées. Cela contredit le principe même de l'indépendance du service de réception des données des assureurs-maladie. Afin de garantir cette indépendance, il faut que des mesures techniques et organisationnelles soient prises. Par exemple, créer deux postes de travail dont les tâches sont totalement séparées ou mettre en place des droits d'accès différents de sorte que l'on ait uniquement accès aux données qui sont effectivement nécessaires pour la tâche en question. Du point de vue organisationnel et technique, cette méthode permet d'empêcher qu'un collaborateur ait accès à toutes les données.

Une autre difficulté d'ordre organisationnel se pose s'agissant de la répartition des tâches: comment gérer conformément à la loi les données confidentielles, réservées au médecin-conseil. Si, au cours de l'examen approfondi des factures transférées par le service de réception des données, il faut requérir des informations supplémentaires de nature médicale (rapports de sortie, rapports d'opération), ces informations sont normalement destinées au médecin-conseil de l'assureur-maladie. Celui-ci procède ensuite à l'évaluation médicale. Toutefois, si des questions concernant le codage doivent être examinées, il doit souvent faire appel au codeur ou au collaborateur DRG du service des prestations lesquelles, du point de vue organisationnel, ne font pas partie du service du médecin-conseil. Dans la pratique, cette difficulté est également résolue par les mesures techniques et organisationnelles mentionnées plus haut.

Ainsi, au cours de nos contrôles, nous avons constaté que certains services de médecin-conseil possèdent des postes de travail séparés qui possèdent une règle d'accès spécifique et prévoient une double fonction pour les collaborateurs, si bien que là aussi, une séparation des deux tâches et de l'accès aux données peut être garantie. En outre, ces collaborateurs à double fonction sont qualifiés d'auxiliaires du médecin-conseil de sorte que lorsqu'ils accomplissent cette tâche pour le médecin-conseil, ils sont soumis au même devoir du secret que le médecin-conseil lui-même (art. 321 CP).

En complément de notre activité de contrôle, plusieurs séances de coordination ont eu lieu au cours de l'année sous revue avec l'Office fédéral de la santé publique (OFSP). Elles avaient pour objet de coordonner des activités de surveillance qui se recoupaient en partie et de clarifier des questions en suspens concernant les services de réception des données.

La séance annuelle avec les certificateurs et avec le Service d'accréditation suisse (SAS) a également eu lieu durant l'année sous revue. Elle a permis un échange de vues constructif et a été l'occasion d'éliminer des points peu clairs, qu'il s'agisse de la certification et de la fonction des services de réception des données ou des interfaces entre les prestataires, les services de réception des données et les assurances-maladie.

Pour conclure, nous constatons que le système des services de réception des données fonctionne bien et que l'application de l'article 59a OAMal, bien qu'il n'y ait eu ni directives concrètes ni prototype d'un service de réception des données, se déroule de manière très satisfaisante et en conformité avec la loi. La concrétisation des services de réception est un processus qui, comme toute autre mise en œuvre d'une nouvelle loi, a besoin de temps afin que nous puissions en déceler les avantages et les inconvénients ainsi que le potentiel d'amélioration. Au cours du prochain exercice, nous procéderons encore à d'autres contrôles et espérons

que s'il faut remédier à des lacunes du point de vue de la protection des données, la collaboration avec les certificateurs, les assurances-maladie et leurs prestataires demeurera fructueuse.

1.6.2 Format d'échange de données XML 4.4 pour les factures DRG

Les données électroniques pour le décompte des prestations hospitalières sont envoyées par l'hôpital à l'assuré, dans une structure définie et avec un contenu donné. Nous avons analysé les factures DRG et constaté que les procédés utilisés s'écartent des dispositions légales.

L'ordonnance sur l'assurance-maladie (OAMal) définit entre autres les données que les hôpitaux doivent fournir aux assureurs pour le décompte des prestations par groupes de diagnostic (DRG). Le Forum Datenaustausch (Echange de données) fournit, pour le transfert électronique des données, un format standardisé qui comprend à la fois la structure et le contenu (métadonnées). Ce standard est appelé XML 4.4. Nous l'avons analysé en détail et il est apparu que les règles utilisées divergeaient des exigences légales. Conformément à l'ordonnance, l'assureur doit recevoir, avec la facture, des enregistrements de données comprenant les données administratives et les données médicales minimales (le MCD) pour pouvoir vérifier la facture conformément à la loi.

Le standard XML 4.4 assemble un fichier de facture (Invoice) et un fichier MCD dans un conteneur XML. Le MCD contient des données médicales et des données administratives. Le conteneur est transféré du prestataire de services à l'assureur. L'inconvénient de cette structure est que l'accès aux données administratives mène automatiquement à une divulgation des données médicales et inversement. La séparation prescrite par la loi entre données administratives et données médicales doit donc être entreprise au bout de la chaîne de traitement, dans les systèmes de l'assureur.

Un autre problème est dû au fait que le code DRG et le diagnostic (codé selon ICD) sont mentionnés dans le XML 4.4 Invoice, donc dans la facture électronique proprement dite. Tous deux sont des informations médicales qui ne doivent pas être mentionnées dans la facture, mais uniquement dans le MCD. Cela a également pour conséquence que l'assureur doit traiter la facture dans son système de telle sorte ni le code DRG, ni le code ICD ne parviennent au service d'encaissement de l'assurance.

Nous avons attiré l'attention du Forum Datenaustausch et de l'Office fédéral de la santé publique sur ce dysfonctionnement et demandé qu'une solution soit trouvée.

À l'avenir, l'ordonnance doit décrire de manière claire ce qu'il doit y avoir dans la facture; la séparation claire entre données médicales et données administratives doit être déjà faite dans les fichiers XML et le code DRG et le code ICD ne doivent pas figurer dans Invoice.

1.6.3 Assurances-maladies complémentaires: effacement des données figurant dans les demandes d'adhésion

Nous avons été informés à plusieurs reprises que quelques assurances-maladies complémentaires n'avaient pas effacé les données concernant la santé de personnes dont la demande d'adhésion n'avait pas abouti à un contrat. Les assurances ont pourtant l'obligation d'effacer spontanément ces données.

Les assurances-maladies complémentaires ne sont pas obligées d'accepter tout le monde. Elles ont le droit de vérifier l'état de santé du demandeur et d'émettre des réserves pour raisons de santé ou de rejeter entièrement la demande. En remplissant et renvoyant le formulaire, le demandeur donne son consentement à ce que l'assurance traite ses données à des fins de vérification. Sur ce formulaire, outre ses données d'identité, il fournit des renseignements sur sa santé et afin de vérifier ces données, les assurances requièrent souvent, par le biais de ce même formulaire, que les médecins traitants soient déliés de leur obligation de garder le secret.

Si l'assurance complémentaire rejette une demande après avoir vérifié les données en question ou si elle émet une réserve, aucun contrat n'est conclu. Dans ce cas, les données demeurent malgré tout auprès de l'assureur. Le demandeur n'a toutefois donné son accord que pour le traitement de ses données dans le cadre de l'examen de sa demande. L'assurance-maladie complémentaire doit donc effacer les données en question, même si elle n'y a pas été invitée expressément. Ces données doivent du reste être traitées avec une attention toute particulière car il s'agit de données sensibles.

Nous avons instamment prié les assureurs qui n'avaient pas effacé les données des demandeurs concernés, même après y avoir été invités, de s'exécuter. Il y a toutefois un certain rapport d'antinomie entre le devoir d'effacement et les intérêts de l'assurance. En effet, l'assurance-maladie complémentaire désire consigner qui a déposé une demande chez elle et pour quelle raison elle l'a refusée afin de ne pas être obligée, si la personne réitère sa demande, de faire à nouveau les mêmes recherches. Nous considérons comme justifié l'intérêt de l'assurance à conserver, pendant un certain temps, dans son système les données d'identification du demandeur ainsi qu'une brève motivation du refus. Par contre, il serait disproportionné de conserver tous les formulaires de demande contenant les renseignements médicaux, ainsi que d'autres informations médicales rassemblées.

1.6.4 Les procurations dans le domaine des assurances

Un certain flou règne à propos des procurations dans le domaine des assurances, notamment lorsqu'elles concernent les données médicales. Nous recevons régulièrement des demandes de la part d'assurés qui s'inquiètent de savoir si la procuration qui leur est soumise ne va pas trop loin. Il serait souhaitable que les assurances introduisent dans ce domaine une pratique uniforme et conforme à la protection des données.

Une procuration est nécessaire lorsque la collecte de données souhaitée par l'assurance n'est pas réglée par la loi. Cela signifie que le médecin ou l'employeur interrogé par l'assurance ne peut communiquer des renseignements sur la santé de la personne en question que s'il dispose d'une procuration.

Bon nombre de personnes sont déstabilisées lorsque, désirant changer de caisse-maladie, elles doivent remplir une procuration alors qu'elles ne le devaient pas auprès de la précédente caisse. Les assurances ont à cet égard des pratiques très différentes.

Les assurances doivent demander une nouvelle procuration pour chaque nouvel événement assuré. En effet, une procuration ne peut se référer à tous les événements futurs. Elle doit nommer l'objet de la recherche, par exemple «sinistre du xx.xx.2015», et elle doit limiter le traitement aux données nécessaires dans ce contexte.

En général, les assurances utilisent des procurations standard qu'elles remettent à tous les assurés au moment de la conclusion du contrat ou de la survenue d'un événement assuré.

Étant donné que la même procuration est souvent utilisée pour des événements différents, de nombreux services peuvent y être cités (médecin traitant, hôpital, employeur, autres assurances, etc.) auprès desquels il est possible de demander des informations. Toutefois, cela ne signifie pas que l'assurance peut se procurer des informations auprès de tous les services nommés. En effet, seuls les traitements de données nécessaires au cas concret sont couverts par le consentement de la personne concernée. En revanche, le service interrogé doit vérifier, malgré la présence d'une procuration, que les données souhaitées sont requises par l'objectif visé et qu'aucun intérêt particulier prépondérant de la personne concernée ne s'oppose à une communication des données.

La pratique a montré qu'en général, les assurances n'acceptent pas que les assurés modifient la procuration et menacent immédiatement d'une réduction des prestations pour non-respect du devoir de collaboration. Dans les faits, les assurés sont obligés de signer la procuration.

Malgré les compétences très larges des assurances concernant les données requises, elles doivent respecter les principes de la protection des données. Afin de dissiper l'incertitude des personnes concernées, il serait souhaitable que les assureurs des différentes branches d'assurance puissent s'accorder sur une pratique uniforme concernant les procurations.

Nous recommandons aux personnes qui veulent savoir quelles données médicales ont été rassemblées à leur sujet de déposer une demande d'accès auprès du service compétent. La procuration peut en outre être révoquée à tout moment.

1.6.5 Communication des données de l'assurance-maladie dans le cadre de la réduction des primes

La communication de l'effectif complet d'assurés aux cantons par la compagnie d'assurance-maladie dans l'optique de la réduction des primes constitue un sujet délicat. La proportionnalité de la communication des données doit être sérieusement mise en doute.

Dans le cadre de la réduction des primes, les assureurs-maladie de l'assurance obligatoire des soins peuvent transmettre aux organes d'exécution cantonaux compétents l'effectif complet des assurés si le droit cantonal prévoit une base juridique pour la communication des données. Par conséquent, les dispositions légales déterminantes ont été adaptées au niveau fédéral.

Quant à nous, nous nous sommes opposés dès le départ à ce projet. Nous émettons en effet des doutes sur le fait que le traitement des données par les organes fédéraux doive entrer dans la sphère de compétences des cantons, et sommes convaincus que la communication de l'effectif complet des assurés viole le principe de proportionnalité. Un très grand nombre des personnes concernées par une telle communication de données n'a pas droit à une réduction des primes ou ne souhaite pas le faire valoir, même s'il existe. Par ailleurs, la plupart des cantons prévoient aujourd'hui encore une procédure de demande spécifique pour les réductions de primes. Cette procédure permet aux services d'exécution cantonaux d'obtenir facilement les informations requises sur la personne assurée.

L'argument selon lequel la communication de l'effectif complet des assurés aux services d'exécution cantonaux simplifie la procédure ne peut justifier la violation du principe de proportionnalité. Ceci est également le cas lorsque l'assurance concernée demande au service d'exécution cantonal de confirmer par écrit que les données sur les assurés ne seront utilisées qu'à des fins de réduction des primes.

1.7 Secteur du travail

1.7.1 Vidéosurveillance dans des établissements de restauration

Cette année, nous avons lancé des procédures d'établissement des faits dans des entreprises de restauration et de vente de plats à l'emporter. Nous tenons à poursuivre notre démarche de sensibilisation aux problématiques relevant du droit de la protection des données dans ce secteur.

On nous a signalé à plusieurs reprises que des établissements de restauration avaient installé des systèmes de vidéosurveillance permettant de surveiller leurs employés de façon constante. Il nous a également été rapporté que des conversations étaient parfois écoutées et enregistrées. Ces informations nous ont incités à clarifier les faits auprès des établissements concernés. Ceux-ci ont répondu à nos questions en nous annonçant que les caméras avaient entretemps été démontées, ce que nos vérifications ont confirmé. Le traitement des données n'étant par conséquent plus effectué, nous avons clos notre contrôle.

Sur la base d'une nouvelle annonce, nous avons ouvert une procédure d'établissement des faits auprès d'une société de restauration à l'emporter. Pour cela, nous avons enquêté aussi bien dans l'entreprise elle-même que chez ses différents partenaires afin de déterminer le type et l'étendue d'éventuelles activités de vidéosurveillance. Là encore, les caméras ont été démontées pendant l'enquête.

Ces cas nous ont montré la nécessité de sensibiliser et d'informer dans le domaine de la vidéosurveillance sur le lieu de travail. C'est la raison pour laquelle d'une part, nous allons préciser nos explications à ce sujet, d'autre part, nous sommes entrés en contact avec l'Inspection fédérale du travail afin de coordonner d'éventuels projets de sensibilisation en la matière. En effet, les enregistrements vidéo pouvant entraîner une surveillance systématique des comportements sont, selon l'ordonnance relative à la loi sur le travail, illicites. Les sanctions en cas de violation de cette ordonnance étant de la compétence des inspections cantonales du travail, nous renvoyons les personnes concernées aussi auprès de ces autorités.

1.7.2 Questionnaire de santé lors d'une candidature

Au cours de l'année sous revue, nous avons examiné à quelles conditions un employeur peut exiger d'un candidat qu'il réponde à un questionnaire sur la santé.

Les données personnelles sur des collaborateurs ne peuvent être traitées que pour autant qu'elles concernent l'adéquation de ces personnes avec un poste déterminé ou qu'elles soient requises pour l'exécution du contrat de travail. Afin de déterminer si un candidat est adapté à un poste donné, l'employeur est également habilité à traiter des informations relatives à la santé. Un tel traitement doit toutefois être proportionné: seules les données nécessaires à la réalisation de l'objectif peuvent être collectées, autrement dit, seules les informations permettant – selon des critères objectifs – de clarifier l'adéquation au poste de travail peuvent être prélevées. En conséquence, l'employeur doit déterminer si un questionnaire de santé est nécessaire pour le poste à pourvoir.

Selon nous, de tels questionnaires ne sauraient être obligatoires de manière générale pour toutes les fonctions. Nous considérons plutôt qu'une telle clarification est nécessaire uniquement pour les postes qui exigent des candidats des compétences particulières – par exemple un besoin en sécurité accru ou des sollicitations physiques particulières. Si une clarification se révèle nécessaire, l'employeur ne peut toutefois se renseigner lui-même sur l'état de santé du candidat. Il peut alors déléguer cette tâche au service médical compétent ou à un médecin-conseil, qui pourront traiter les données requises pour déterminer l'adéquation au poste en question. Ils indiqueront ensuite à l'employeur si le candidat est adapté au poste à pourvoir, sans lui communiquer toutefois de diagnostic.

On peut donc dire pour résumer que l'admissibilité d'un tel questionnaire dépend du poste ou de la fonction. Si un candidat doit remplir un questionnaire, il doit certes indiquer ses pathologies (p. ex. diabète), mais le médecin ne peut communiquer aucun diagnostic à l'employeur. Il ne peut que l'informer d'une adéquation insuffisante pour le poste concerné, par exemple si la maladie compromet directement et actuellement la capacité de travail ou empêche la réalisation des tâches prévues.

1.7.3 Arrêt du Tribunal administratif fédéral concernant le bureau de communication pour lanceurs d'alerte (Whistleblowing)

Dans son arrêt concernant le bureau de communication pour lanceurs d'alerte (Whistleblowing) du Contrôle fédéral des finances, le Tribunal administratif fédéral a admis toutes nos conclusions.

Comme indiqué dans notre dernier rapport d'activités (2013/2014, ch. 1.7.2), nous avons procédé à un examen des faits auprès du Contrôle fédéral des finances (CDF), et avons sur cette base émis une recommandation selon laquelle il devait nous déclarer ses fichiers et établir un règlement de traitement conformément

à la législation sur la protection des données. Le CDF n'a pas voulu suivre notre recommandation, de sorte que nous avons porté l'affaire devant le Tribunal administratif fédéral (TAF). Celui-ci a, par jugement du 16 décembre 2014, pleinement donné suite à nos demandes (cf. A-788/2014). Le TAF a d'abord rappelé la définition des données personnelles et conclu que le CDF traitait de telles informations. Il est ensuite revenu sur les commentaires relatifs aux fichiers selon le message concernant la loi fédérale sur la protection des données (LPD), estimant que l'interprétation large de la définition légale de fichier (selon laquelle tout ensemble de documents stockés sous forme électronique constituerait généralement un fichier) était critiquée à juste titre dans les textes de référence. Le TAF estime toutefois que la catégorisation des données est tout à fait possible car il s'agit finalement d'enregistrer des annonces se fondant sur l'art. 22a de la loi fédérale sur le personnel de la Confédération. Le fait qu'il ne s'agisse pas pour le CDF de procéder à un traitement des données en tant que tel mais simplement à un stockage interne n'y change rien.

Concernant la possibilité d'identification, le Tribunal signale que les noms de personnes et d'autres indications seraient enregistrés par le CDF (pour autant que les renseignements ne soient pas anonymes). Par conséquent, la fonction de recherche dans les documents permettrait de trouver des données personnelles sans que des connaissances techniques particulières ne soient requises. Pour ces raisons, le Tribunal administratif fédéral a confirmé notre conclusion selon laquelle les enregistrements du bureau de communication pour lanceurs d'alerte constituaient des fichiers.

Selon le TAF, il n'est pas exclu que les fichiers décrits qui sont concernés ici contiennent également des données sensibles, à savoir des données sur la santé, des mesures administratives ou pénales, ou encore certaines opinions et activités. Le CDF doit donc rédiger un règlement de traitement répondant aux exigences énoncées à l'art. 21, al. 2 OLPD. Du point de vue de la proportionnalité, l'établissement de ce règlement serait également approprié car aucune ordonnance d'exécution n'est exigée. L'obligation d'élaborer un règlement de traitement serait également raisonnable en termes de coûts, et ne représenterait pas une mesure radicale.

Pour résumer, le Tribunal administratif fédéral a estimé que nos demandes étaient justifiées et a admis notre action en justice et nos conclusions. En conséquence, le CDF est tenu de nous déclarer ses deux fichiers conformément à l'art. 11a, al. 2 LPD dans un délai de deux mois après l'entrée en force de ce jugement et est chargé de rédiger un règlement de traitement au sens de l'art. 21 OLPD pour le traitement des données dans ces deux fichiers. Le CDF n'entend cependant pas accepter le jugement et a déposé un recours auprès du Tribunal fédéral.

1.7.4 Communication de renseignements dans le cadre d'une postulation

Notre service de renseignement téléphonique a reçu de nombreux appels concernant les renseignements fournis par de précédents employeurs dans le cadre d'une postulation. Apparemment, il règne une certaine incertitude s'agissant des droits du candidat dans ce contexte et de ses moyens de défense contre des renseignements fournis sans autorisation ou ne correspondant pas à la réalité.

Au cours de l'année sous revue, nous avons à nouveau reçu de nombreux appels concernant l'octroi de renseignements sur un candidat par ses précédents employeurs. Nous avons informé les personnes concernées que les principes fondamentaux de la loi fédérale sur la protection des données (LPD) sont dans ce cas applicables. La demande et l'octroi de renseignements doivent se faire dans le respect des principes de licéité, de la bonne foi et de la proportionnalité. En d'autres termes, un employeur ne doit demander ou transmettre que les informations qui sont pertinentes dans la perspective du futur poste ou nécessaires à la mise en œuvre du contrat de travail. Dans ce contexte, les traits essentiels de la personnalité de l'employé sont inévitablement jugés. En vertu de la LPD, il s'agit là de profils de personnalité et leur traitement nécessite le consentement préalable et explicite de la personne concernée. On ne saurait donc simplement supposer que ce consentement a été donné parce que, par exemple, le candidat a donné la liste de ses précédents employeurs dans son curriculum vitae. Par contre, si un dossier de candidature indique à la rubrique «Références» les coordonnées d'un ancien employeur ou d'un ancien supérieur, cela peut être considéré comme consentement ou acceptation de la part du candidat en vue d'une prise de contact avec l'employeur.

L'ancien employeur, à qui on demande des informations sur le candidat, doit s'assurer avant que celui-ci a donné son consentement. Il n'est pas obligé de s'adresser pour cela directement au candidat; le consentement peut aussi être confirmé si l'ancien employeur a la possibilité de consulter la liste de références transmise par le candidat. En outre, le candidat a le droit d'être informé par l'ancien employeur qu'il a donné comme référence si celui-ci a transmis des renseignements, à qui et quel en était le contenu.

L'octroi d'un renseignement non autorisé constitue une atteinte illicite à la personnalité. Conformément à l'art. 15 LPD, la personne concernée peut intenter une action civile contre l'atteinte ainsi portée à sa personnalité ou contre le traitement sans motif justificatif de ses données personnelles. Conformément à l'art. 35 LPD, le candidat concerné a en outre la possibilité d'engager des poursuites pénales contre

son ancien employeur si celui-ci a communiqué des données sensibles ou un profil de la personnalité sans son consentement.

Les renseignements pris auprès d'un employeur à propos du candidat servent principalement à approfondir l'impression qui se dégage d'un certificat de travail. Donc, tout comme dans le cas d'un certificat, le principe général est le suivant: les informations données doivent être objectives, véridiques et en même temps bienveillantes. Les renseignements fournis ne doivent pas entraver l'avenir économique de l'ancien employé, ni enfreindre le devoir de sollicitude de l'employeur, qui comprend la protection de la personnalité de l'employé. Le devoir de sollicitude ne vaut pas seulement pendant la durée de la relation de travail, mais dans une certaine mesure aussi au-delà de la période d'engagement. Si l'ancien employeur enfreint son devoir de sollicitude prévu par le droit du travail, le candidat concerné peut non seulement intenter une action pour atteinte à la personnalité, mais aussi faire valoir des dommages éventuels et un tort moral.

Concrètement, le candidat concerné peut faire cesser par le biais d'une action civile les informations fausses et trompeuses qui ont porté atteinte à sa personnalité. S'il a dû subir un dommage concret en raison de la fausse déclaration de son ancien employeur, s'il n'a pas obtenu un emploi en raison de ces informations fausses et trompeuses, il peut en outre demander des dommages et intérêts et réparation de tort moral. Cela nécessite toutefois un rapport direct entre les informations et la décision du nouvel employeur potentiel. Dans la réalité, il est difficile d'apporter cette preuve. Nous recommandons donc aux candidats concernés de se faire conseiller du point de vue juridique avant d'intenter une action en justice.

1.7.5 Transmission de données dans le domaine des mesures d'accompagnement

Nous avons analysé sous l'angle juridique de la protection des données la problématique du traitement et de la transmission de données dans le domaine des mesures d'accompagnement de la loi sur les travailleurs détachés.

Cette année, nous avons été souvent sollicités par des entreprises agissant comme sous-traitants sur de gros chantiers pour déterminer si et dans quelle mesure la communication des données de leurs collaborateurs aux entreprises générales était licite. Sur la base de ces requêtes, nous avons examiné avec attention les transmissions de données prévues dans le cadre de contrôles au sens de la loi sur les travailleurs détachés. Pour ce faire, nous avons également pris contact avec le Secrétariat d'État à l'économie afin de mieux comprendre les différents processus de contrôle dans ce domaine. Nos vérifications nous ont permis de conclure

que les données personnelles des collaborateurs des sous-traitants pouvaient être transmises en cas de responsabilité solidaire ou de contrôles prévus par la loi sur les travailleurs détachés. Cependant, le principe de proportionnalité doit toujours être respecté, ce qui signifie que seules les données nécessaires à la réalisation de l'objectif prévu peuvent être transmises.

1.8 Économie et commerce

1.8.1 Smart grids et protection des données

Nous avons apporté nos conseils à l'Office fédéral de l'énergie dans le cadre de la préparation à l'introduction étendue des systèmes de mesure intelligents.

Dans l'année sous revue, nous avons apporté nos conseils au groupe de travail de l'Office fédéral de l'énergie (OFE) en matière de systèmes de mesure intelligents (compteurs numériques) et de protection des données. L'étude du groupe de travail a été publiée sur le site Internet de l'OFE (www.bfe.admin.ch/smartgrids). Selon cette étude, il serait pertinent de prévoir une réglementation uniforme au niveau fédéral ou l'application de la loi fédérale sur la protection des données dans le domaine de l'exploitation des réseaux intelligents (smart grids). L'OFE nous a priés de le soutenir dans l'élaboration d'un éventuel règlement du traitement des données des compteurs intelligents (smart metering) à l'échelle de la Suisse.

1.8.2 Cartes clients dans le commerce de détail

Les contrôles complets réalisés dans le domaine des cartes clients de Migros et de Coop se sont poursuivis cette année, et nos évaluations juridiques sur le plan de la protection des données ont été consignées dans des rapports.

L'année dernière, nous avons effectué des contrôles a posteriori sur le thème des cartes clients des grands distributeurs Migros et Coop (cf. notre 21e rapport d'activités 2013/2014, ch. 1.8.2). Les contrôles réalisés auprès de Migros ont montré que la société est consciente des risques en matière de droit de la protection des données et s'efforce de les minimiser par des mesures appropriées. C'est pourquoi le rapport dresse un tableau globalement positif concernant l'évaluation des traitements de données. Nous avons cependant également constaté que diverses améliorations étaient encore nécessaires sur le plan de l'information et de la transparence, et nous avons formulé des propositions dans ce sens.

En outre, nous avons émis une recommandation formelle selon laquelle Migros doit indiquer, dans le cadre d'une demande fondée sur le droit d'accès, dans quel segment le client est classé sur la base des analyses liées aux données clients. Cette classification représente une composante centrale du traitement des données. Et la communication à toute personne concernée de la manière dont elle est classée selon les données collectées par l'entreprise est indispensable pour que cette personne puisse se faire une idée des critères d'analyse, évaluer leur exactitude et se comporter en conséquence. Migros a accepté toutes nos propositions

d'amélioration ainsi que la recommandation, et les applique en conséquence ou les a déjà mises en œuvre.

De même, un rapport concernant la carte de fidélité a été adressé à Coop pour prise de position. Cependant, les contrôles n'ont pas encore pu être clos car il subsiste certaines divergences par rapport à nos appréciations.

1.8.3 Recherches dans le domaine des agences de renseignement économique et de renseignement en matière de crédit

Au cours de l'année sous revue, nous avons clos notre second examen des faits concernant la conformité à la protection des données de la prestation fournie par la plateforme www.moneyhouse.ch et émis une recommandation.

Durant l'année sous revue, nous avons terminé la seconde partie de notre examen concernant la plateforme www.moneyhouse.ch et nous avons émis un certain nombre de recommandations dans notre rapport final. Depuis le début de notre dernier établissement des faits (cf. notre 21e rapport d'activités 2013/2014, ch. 1.8.5), itonex AG n'a cessé d'élargir l'offre des prestations accessibles par l'intermédiaire de www.moneyhouse.ch. Outre la consultation d'informations provenant du registre du commerce, il est également possible de conclure des abonnements concernant la solvabilité, le comportement en matière de paiement et le recouvrement des créances et d'obtenir en outre des informations concernant des demandes de permis de construire et leur octroi ou concernant des offres d'emplois. Nous avons donc conclu dans notre rapport final qu'itonex AG traitait des profils de la personnalité. Le traitement de profils de la personnalité comportant de grands risques pour les personnes concernées, la loi fédérale sur la protection des données (LPD) prévoit à cet égard des prescriptions spécifiques. La transmission de renseignements sur la solvabilité, prestation que fournit itonex AG, est dans ce contexte problématique. En effet, une société fournissant des renseignements sur la solvabilité ne peut traiter des profils de la personnalité.

Sous l'angle de la protection des données, nous avons également décelé d'autres problèmes, touchant spécialement le traitement de données concernant des enfants et la possibilité d'accéder aux données du registre du commerce par le biais des moteurs de recherche (cf. notre présent rapport d'activités, ch. 1.1.3). De même, nous avons demandé de garantir que les données personnelles mises en relation soient justes et que les contenus effacés ne soient pas rétablis. Au début de l'année 2015, itonex AG a partiellement accepté notre recommandation (cf. www.leprepose.ch – protection des données – documentation – recommandations). Les points sur lesquels il n'a pas été possible de trouver un accord seront soumis au Tribunal administratif fédéral, afin de clarifier la situation juridique.

1.8.4 Mise en œuvre du droit d'accès et du droit d'opposition par des maîtres de fichier

Suite à de nombreuses plaintes de particuliers qui avaient fait valoir leur droit d'accès, nous avons écrit aux maîtres de fichier concernés pour les rendre attentifs à la situation légale et leur rappeler leurs obligations. Dans un cas, nous avons émis une recommandation.

Conformément à la loi fédérale sur la protection des données (LPD), toute personne peut faire valoir son droit d'accès auprès du maître d'un fichier. Celui-ci doit en particulier lui communiquer toutes les données la concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données. Les renseignements doivent être fournis gratuitement et par écrit dans un délai de trente jours. Le droit d'accès ne peut être ajourné, restreint ou refusé que si des intérêts prépondérants s'y opposent. Dans ce cas, le maître de fichier doit motiver son refus. De plus, toute personne peut exiger l'effacement de ses données personnelles si aucun motif justificatif n'en justifie le traitement.

Nous recevons régulièrement des plaintes concernant des sociétés qui ne répondent pas aux demandes de droit d'accès et d'opposition alors qu'elles y sont légalement tenues. Nous avons en particulier reçu un certain nombre de réclamations concernant deux sociétés, à savoir une maison d'édition et un commerçant d'adresses. Sur la base de nos compétences en matière de surveillance et vu le nombre de cas concernés, nous avons écrit à ces sociétés afin de leur rappeler leurs obligations découlant de la loi sur la protection des données. Dans un cas, nous avons émis une recommandation formelle.

Nous avons publié la recommandation sur notre site www.leprepose.ch sous la rubrique Protection des données – Documents – Recommandations (en langue allemande uniquement)

1.8.5 Communication de données de membres à des assurances

Cette année encore, nous avons reçu des demandes de particuliers qui demandaient dans quelle mesure les associations sportives pouvaient communiquer leurs données de membres à des sponsors à des fins de démarchage publicitaire. Nous allons contacter les fédérations et les deux sponsors principalement concernés afin de les rendre attentifs à la situation légale en matière de protection des données.

Nous continuons de recevoir des demandes de particuliers ou de clubs sportifs concernant la communication de données de membres à des assurances à des fins de démarchage publicitaire (cf. notre 16e rapport d'activités 2008/2009, ch. 1.8.5 et notre 17e rapport d'activités 2009/2010, ch.1.8.4). Rappelons qu'une association sportive ne peut – même ponctuellement – communiquer à des tiers les adresses de ses membres à des fins de marketing que si elle dispose du consentement des personnes concernées. Le consentement doit être libre et éclairé mais, concernant de simples adresses, peut être implicite, par exemple lorsqu'une telle utilisation des données de membres est prévue par les statuts et que les membres ne s'y sont pas opposés.

Nous avons pu constater que, de plus en plus fréquemment, ce sont les fédérations qui communiquent aux sponsors les données des membres individuels. Les données sont le plus souvent transmises par les clubs dans le cadre de l'attribution d'une licence ou à d'autres fins administratives. La fédération peut bien prévoir, par exemple dans ses statuts, que les données de ses propres membres seront communiquées à ses sponsors (les membres doivent cependant avoir la possibilité de s'y opposer). La fédération ne peut toutefois sur cette base communiquer les données des autres sportifs. Une communication à des fins de prospection publicitaire de données qui ont été transmises à la fédération à des fins administratives (obtention d'une licence, par exemple) viole le principe de finalité et est, sauf motif justificatif, illicite.

Concrètement, pour que la communication des données à ses sponsors soit licite, la fédération devra s'assurer qu'elle dispose du consentement des personnes concernées, à savoir les membres des clubs. Si elle ne dispose pas d'un consentement valable, alors toute communication à des sponsors est illicite. Dans tous les cas, les membres doivent avoir la possibilité de s'opposer à une telle utilisation de leurs données. Nous allons contacter les fédérations afin de leur indiquer la situation juridique et leurs obligations en matière de traitement des données.

Les sponsors, quant à eux, doivent également s'assurer (au moins par contrat) que les adresses transmises peuvent être utilisées à des fins de prospection publicitaire. Nous avons constaté que la plupart des cas rapportés concernaient deux assurances en particulier. Nous allons écrire à ces dernières afin de les rendre attentives à la situation légale en matière de protection des données, afin qu'elles en tiennent compte dans les contrats de sponsoring.

1.9 Finances

1.9.1 Clarifications relatives au traitement de données client chez Postfinance

Postfinance a lancé fin 2014 une nouvelle version de sa plateforme de banque électronique. Les clients sont invités à accepter les nouvelles dispositions de participation, sans quoi ils perdent leur accès électronique. Nous évaluons actuellement les traitements de données dans le cadre d'un examen des faits.

Début 2014, Postfinance nous a communiqué pour la première fois son intention de remanier sa plateforme de banque électronique (e-banking). Nous avons été informés du projet au travers de deux séances et de diverses documentations. Postfinance nous a priés de procéder à une évaluation sous l'angle du droit de la protection des données car la révision de sa plateforme implique de nouveaux traitements de données. Nous avons donc envoyé à Postfinance une prise de position détaillée, mais n'avons pas reçu de commentaires à cet égard.

A partir d'août 2014, Postfinance a informé ses clients, sur une page intermédiaire de sa plateforme d'e-banking accessible après connexion, de l'introduction de la version révisée et des nouveautés qu'elle entraîne. Un logiciel d'analyse est notamment obligatoire pour tous les clients afin d'assurer la planification du budget et la représentation des flux monétaires. En outre, l'analyse des transactions permet aux clients de Postfinance de recevoir des offres spéciales d'entreprises tierces sur leur page e-banking. Les clients ont été invités à accepter les nouvelles conditions de participation pour pouvoir continuer à utiliser leur accès électronique. Sur la base de cet état de fait et de nombreuses annonces de citoyens, nous avons décidé d'ouvrir un examen des faits afin d'analyser les traitements de données. Postfinance a accepté les propositions d'amélioration que nous lui avons soumises dans ce contexte et a assuré qu'elle allait adapter la plateforme d'e-banking en conséquence: les clients seront mieux informés et auront désormais la possibilité de choisir; aucune analyse ne pourra être effectué sans leur consentement.

1.9.2 Consultation en vue de l'échange automatique de renseignements fiscaux

Suite à l'introduction du nouveau standard international de l'OCDE régissant l'échange automatique de renseignements en matière fiscale, nous avons été invités à participer aux groupes de travail mis sur pied par le Secrétariat d'État aux questions financières internationales (SFI). Dans le cadre de cette consultation, nous avons eu l'occasion d'attirer l'attention du SFI sur des questions centrales en matière de droits de la personnalité.

Durant l'année sous revue, diverses tables rondes ont eu lieu, afin notamment de préparer la loi d'application en droit interne qui réglementera l'échange automatique de données fiscales. Le plan de route est ambitieux, étant donné que la Confédération entend collecter des données dès 2017 et entamer les échanges avec les États partenaires à partir de 2018. Entre-temps, les accords et la loi d'application devront être prêts et entrés en vigueur sans quoi les échanges ne pourront débuter, faute de base légale.

Dans le cadre de ces travaux, la question de la protection des données est au centre du débat. Nous avons dès lors eu l'occasion de nous exprimer sur plusieurs points importants avant et pendant la consultation des offices. Un des griefs notamment soulevé concerne le projet d'utiliser le numéro AVS pour en faire un numéro d'identification fiscale (NIF), qui serait traité également à l'étranger. Une telle utilisation de ce numéro d'assurances sociales serait en contradiction avec les finalités initiales pour lesquelles il a été conçu et serait de surcroît risqué. Nous avons par conséquent attiré l'attention du SFI sur les risques considérables qu'une telle mesure aurait pour la protection de la personnalité. En effet, l'utilisation du numéro AVS en dehors des assurances sociales rendrait possible un appariement non autorisé de données par des moyens techniques. L'on pense, en l'espèce, spécifiquement aux interconnexions de bases de données par des algorithmes d'une efficacité grandissante. Un numéro d'identification universel, comme le numéro AVS, rend l'interconnexion encore plus simple. Cela permet notamment de créer des profils de la personnalité, d'usurper des identités, etc. Nous avons dès lors plaidé en faveur de l'élaboration d'un numéro sectoriel, à savoir d'un NIF indépendant du numéro AVS, à l'instar de plusieurs États européens déjà au bénéfice d'un numéro sectoriel fiscal.

Suite à nos remarques ainsi qu'à celles de l'Office fédéral des assurances sociales (OFAS), le Département fédéral des finances (DFF) a décidé de faire l'impasse sur l'utilisation du numéro AVS dans le cadre de l'échange automatique de renseignements fiscaux. En outre, nous avons été intransigeants sur le respect des principes de la transparence et de la bonne foi dans le cadre de la procédure d'échange

automatique de renseignements. Nous avons requis que les principes fondamentaux de la protection des données soient pris en compte. Ces principes ont été thématisés dans l'avis du Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe du 4 juin 2014. Ledit document est également cité par le groupe de travail «article 29» dans sa lettre du 18 septembre 2014 à l'attention de l'OCDE et dans laquelle il est en substance requis que les principes soient respectés et mis en oeuvre à la lumière du droit interne de chaque État lors de l'application de la procédure d'échange automatique.

Le respect des droits fondamentaux des justiciables constitue la pierre angulaire de notre engagement dans ce projet. Dès lors, nous mettons tout en œuvre afin que les personnes qui feront l'objet d'une déclaration puissent, en tout état de cause, être entendues et faire valoir leurs droits découlant notamment de la loi sur la protection des données (LPD) en temps utile, à savoir avant de subir un préjudice, par exemple parce que des données erronées auraient été transmises à l'étranger.

1.9.3 Clôture de l'établissement des faits relatif au système de gestion des risques d'un institut financier

La procédure d'établissement des faits en relation avec l'exploitation du système de gestion des risques d'un institut financier est désormais close. Toutes nos recommandations ont été acceptées.

En 2012, nous avions ouvert une procédure d'établissement des faits en relation avec l'exploitation du système de gestion des risques d'un institut financier actif sur la scène internationale. Au terme de la procédure d'établissement des faits (cf. notre 20e rapport d'activités 2012/2013, ch. 1.8.7 et notre 21e rapport d'activités 2013/2014, ch. 1.9.1), nous avons conclu que la mise en œuvre opérationnelle dudit système correspond aux obligations légales découlant du droit bancaire. Le traitement de données est dès lors justifié dans le cas d'espèce. Au niveau du droit de la protection des données, des manquements ont toutefois été identifiés.

Ceux-ci ont notamment trait à l'absence de transparence des traitements effectués. Nous avons donc recommandé à l'institut financier d'attirer l'attention du public de manière générale sur le but et l'utilisation du système et d'informer spécifiquement les personnes concernées par un traitement. Il doit de surcroît procéder à des modifications du système afin de respecter le principe de la proportionnalité du traitement d'un point de vue temporel, c'est-à-dire en matière d'effacement des données après un certain délai.

Nos recommandations ont été acceptées le 28 août 2014 et le rapport final est publié sur notre site (www.leprepose.ch, protection des données – commerce et économie – finances).

1.9.4 Externalisation à l'étranger de données bancaires pseudonymisées

Dans le cadre de la consultation organisée en 2013 par l'Autorité fédérale de surveillance des marchés financiers (FINMA) concernant la révision partielle de la circulaire 2008/21 «Risques opérationnels – banques», nous avons explicité notre position concernant la qualification juridique des données pseudonymisées et de ses conséquences dans le domaine bancaire.

Au cours de l'année sous revue, la FINMA a attiré notre attention sur les divergences entre la mise en œuvre pratique de la circulaire 2008/7 de la FINMA «Outsourcing – banques» et la position du PFPDT. En Suisse, une grande partie des instituts financiers surveillés estiment qu'il n'est pas obligatoire d'informer spécifiquement les clients sur l'externalisation de leurs données personnelles lorsque celles-ci sont pseudonymisées. Les représentants de la branche sont en effet d'avis que ces données ne relèvent pas de la loi fédérale sur la protection des données (LPD).

Cette position repose sur une interprétation divergente de la qualification juridique de données pseudonymisées. La LPD prévoit que toutes les informations qui se rapportent à une personne identifiée ou identifiable sont des données personnelles. Les représentants du secteur financier estiment que les données pseudonymisées ne peuvent pas être considérées comme des données personnelles. En effet, ils considèrent les données du point de vue du destinataire des données pseudonymisées qui lui, n'est pas en possession des indications nécessaires pour relier les données à une personne et procéder ainsi à une ré-identification. Si l'on suivait cette interprétation, cela aurait pour résultat que l'on pourrait contourner la loi sur la protection des données simplement par le biais de mesures techniques, ce qui est incompatible avec la volonté du législateur.

Il faut partir de définitions claires si l'on veut comprendre la situation d'un point de vue technique. La «pseudonymisation» est procédé spécifique par lequel les éléments permettant une identification directe sont remplacés par un identifiant neutre, en l'occurrence un pseudonyme. Ce pseudonyme est enregistré dans un tableau de correspondance séparé avec les éléments d'identification et permet aux ayants droit d'établir un lien avec la personne concernée qui, de ce fait, est identifiable conformément à la LPD. Cette méthode a pour conséquence que les données ainsi pseudonymisées peuvent être considérées comme non identifiables

pour toutes les personnes qui n'ont pas accès au tableau de correspondance. Bien que par ce processus de pseudonymisation, le lien direct avec une personne est éliminé pour quelqu'un qui ne possède pas de possibilités d'identification, une personne reste identifiable pour le détenteur du tableau de correspondance.

Dans ce cas, une banque par exemple peut conserver son tableau de correspondance en Suisse et externaliser à l'étranger le traitement des données de ses clients après pseudonymisation. Se pose donc la question de savoir à partir de quel point de vue il convient d'apprécier la possibilité d'identifier les personnes concernées: exclusivement du point de vue du destinataire des données (variante A)? Exclusivement du point de vue du fournisseur des données (variante B)? Ou de façon alternative (variante C)? La LPD est applicable ou non selon le point de vue choisi.

Dans la variante A, on se place du point de vue du destinataire des données pour lequel une ré-identification n'est plus guère possible. Les informations externalisées ne peuvent pas être qualifiées, de son point de vue, de données personnelles. La LPD n'est donc dans ce cas pas applicable. Dans la variante B, on parvient à la conclusion contraire. Dans la variante C, on part d'un point de vue alternatif, à savoir ou bien le point de vue de la banque qui externalise, ou celui du destinataire des données. Dans ce cas, la LPD est toujours applicable.

La LPD elle-même ne mentionne pas expressément quelle base d'appréciation appliquer. Toutefois, le législateur était conscient du potentiel considérable de développement de la technique dans le domaine numérique. Il a donc créé une loi techniquement neutre devant permettre de suivre l'évolution de la technologie moderne. En outre, le Tribunal fédéral a confirmé notre position dans l'arrêt Logistep (ATF 136 II 508; cf. notre 18e rapport d'activités 2010/2011, ch. 1.3.5). Dans cet arrêt, le Tribunal fédéral établit les conditions précisant de quel point de vue l'appréciation de l'identifiabilité doit avoir lieu et applique à cet égard l'approche dite «alternative».

Il ressort de ce qui précède que la LPD est applicable dans le cas de l'externalisation à l'étranger de données de clients de banques, ce qui implique certaines obligations pour les banques qui externalisent. Selon la circulaire de la FINMA 2008/7 (Cm 35), le client doit être informé d'une externalisation par courrier spécial et de manière détaillée. En outre, dans cette situation, il doit avoir la possibilité de refuser la clause litigieuse (opt-out ou option de retrait) ou de rompre la relation contractuelle, cela sans subir de préjudice. Nous estimons qu'actuellement, ces règles sont contraignantes dans le domaine de la circulation électronique de données financières où le risque accru de manipulation des données ou d'accès non autorisé de tiers est doit être pris en considération. Il découle en outre de cette approche fondée sur les risques qu'il relève de la responsabilité des instituts financiers de garantir la transparence de ce type de traitement à l'égard des clients afin que ceux-ci puissent faire valoir sans entrave leurs droits à l'autodétermination en matière d'information

La LPD ne fixe aucune contrainte pour ce qui est du support d'information. Il est possible de fournir des informations concernant les risques de l'externalisation dans les conditions générales de la banque, à condition que les clients soient également informés explicitement d'une autre manière et qu'il n'y ait pas d'intégration globale des conditions générales dans le contrat. Comme mentionné plus haut, le client doit avoir la possibilité de se prévaloir d'une option de retrait (opt-out): la banque doit dans ce cas octroyer au client un délai approprié dans lequel il pourra écarter la clause litigieuse ou dénoncer son contrat sans préjudice. Dans le cas contraire, il ne saurait y avoir de consentement libre et éclairé. Si le client n'effectue pas une option de retrait dans le délai fixé, on peut partir de l'idée qu'il a tacitement consenti à l'externalisation. Si des données personnelles sensibles ou des profils de la personnalité sont concernées par l'externalisation à l'étranger, le consentement explicite du client est nécessaire (opt-in, option d'adhésion). Tant que ce dernier n'est pas effectif, la clause d'externalisation n'est pas valable

.

1.10 International

1.10.1 Coopération internationale

Dans un monde globalisé et interconnecté, la coopération internationale demeure une activité incontournable des autorités de protection des données. Comme les années précédentes, l'année a été marquée par les réformes en cours du droit à la protection des données au sein de l'Union européenne et du Conseil de l'Europe. Le renforcement de la coopération internationale est au programme non seulement des autorités européennes de protection des données, mais également de la conférence internationale des commissaires à la protection des données ou de l'Association francophone des autorités de protection des données.

Conseil de l'Europe

La modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) demeure une activité prioritaire et centrale du Conseil de l'Europe. Elle a franchi une étape importante avec l'adoption par le comité ad hoc de protection des données (CAHDATA) d'un projet d'amendement de la Convention, qui reprend dans l'ensemble les propositions faites par le comité consultatif de la Convention 108 (T-PD) (voir notre 20e rapport d'activités 2012/2013, ch. 1.9.1). Le texte sera transmis au Comité des Ministres pour adoption finale et ouverture à l'acceptation des Parties à la Convention. Toutefois, les travaux pourraient être sérieusement ralentis du fait que la Commission européenne a formulé de nombreuses réserves. La Russie, mais cela était attendu, a pour sa part fait deux réserves, l'une portant sur les dispositions régissant les flux transfrontières et préservant le régime de l'Union européenne (décision d'adéquation), l'autre sur les compétences de vote qui seront attribuées à la Commission au détriment des États membres de l'UE.

L'attitude de la Commission européenne, imposant un nombre élevé de réserves au motif qu'il n'y avait pas encore de position commune au sein de l'UE et que celle-ci n'avait pas encore achevé l'examen de la réforme de son cadre juridique en matière de protection des données, a heurté plusieurs délégations. La Suisse a d'ailleurs officiellement fait part de son désappointement. Ces réserves ont pour conséquence que le texte ne pourra vraisemblablement pas être adopté durant le premier semestre 2015 par le Comité des Ministres comme cela avait été initialement planifié. Il faudra vraisemblablement attendre l'adoption des textes européens, qui interviendra au plus tôt à fin 2015, pour pouvoir débloquer la situation.

Ce retard a des conséquences sur le plan interne, car il risque de retarder les travaux de révision de notre législation sur la protection des données. Il donne

également un mauvais signal aux États tiers qui souhaitaient entamer leur processus d'adhésion à la Convention 108. Plusieurs de ces États ont pris part aux travaux du CAHDATA.

Le texte de la modernisation assure et continuera d'assurer la convergence avec les textes européens et les deux cadres juridiques demeureront complémentaires. Retarder l'adoption du texte de la Convention modernisée risque de remettre en cause la politique de promotion de la convention et de décourager les États tiers à y adhérer, donc d'affaiblir le droit à la protection des données en Europe et dans le monde.

Pour sa part, le T-PD a finalisé la révision de la recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (voir 21e rapport d'activités 2013 /2014, ch. 1.10.1), qui devrait être adoptée par le Comité des Ministres en 2015.

Le T-PD a pris connaissance d'un rapport d'experts sur les implications, pour la protection des données, d'un recours croissant à des mécanismes d'échange interétatique et automatique de données à caractère personnel à des fins administratives et fiscales, ainsi que dans le cadre de la lutte contre le blanchiment d'argent, le financement du terrorisme et la corruption, et a autorisé sa publication sur le site du Conseil de l'Europe. Il a en outre adopté à l'unanimité des parties présentes un avis sur les implications en matière de protection des données à caractère personnel des mécanismes d'échange interétatique et automatique de données à des fins administratives et fiscales. Cet avis a été adressé à l'OCDE et aux autorités nationales en charge de cette problématique. L'avis, qui sera rendu public, insiste sur la nécessité du respect des exigences de protection des données découlant de la Convention 108 et du droit à la vie privée de l'article 8 de la Convention européenne des droits de l'homme.

Des garanties spécifiques doivent être adoptées pour assurer le respect des droits fondamentaux des individus dans le cadre de la mise en place de ces mécanismes. Il s'agit en particulier de minimiser les risques d'atteinte à la vie privée et de mesures discriminatoires qui pourraient être prises à l'encontre des personnes concernées. À cet égard, les conventions et accords établis aux fins d'organiser ces échanges devraient être rédigés de manière claire et non équivoque. Il s'agit notamment de définir avec précision le champ d'application, les termes utilisés, les catégories concrètes de personnes concernées, les finalités de la collecte et du traitement, les données traitées et échangées, de désigner l'autorité nationale habilitée à obtenir et traiter ces données. Il convient également d'édicter les règles régissant la conservation des données, de préciser les modalités pratiques de l'échange automatique, de prévoir des règles régissant la transmission des données à d'autres instances

nationales, ou encore de définir les voies de recours dont disposent les personnes concernées.

Le T-PD a également adopté un avis relatif à une recommandation de l'Assemblée parlementaire du Conseil de l'Europe visant à améliorer la protection et la sécurité des utilisateurs dans le cyberespace. Cet avis soutient l'initiative de l'Assemblée parlementaire du Conseil de l'Europe. Il souligne que la garantie de l'effectivité des droits de l'homme dans le cyberespace comprend notamment la promotion des principes universels de protection des données à caractère personnel et le rappel de l'obligation positive des États membres d'assurer une protection juridique adéquate relative à l'interception, à la surveillance, au profilage et à l'archivage des données des utilisateurs. L'élaboration d'un protocole additionnel à la convention sur la cybercriminalité pour les violations graves des droits fondamentaux des utilisateurs de services en ligne passe pour le T-PD par le respect du droit fondamental à la vie privée protégé par l'article 8 CEDH et de la Convention 108 et de son protocole additionnel. À cet égard le T-PD exprime le souhait que les États ratifiant ou adhérant à la convention sur le cybercrime adhèrent également à la convention 108 et son protocole additionnel.

Par ailleurs, le T-PD a entamé des réflexions concernant la protection des données à l'heure des métadonnées. Il a enfin réélu le préposé fédéral suppléant à sa présidence pour un 3e mandat consécutif.

Conférence européenne des commissaires à la protection des données

La conférence européenne des commissaires à la protection des données a été organisée par la Commission française de l'informatique et des libertés (CNIL) et par le Conseil de l'Europe. Elle s'est tenue à Strasbourg le 5 juin 2014. Le thème retenu pour cette conférence a été la coopération entre les autorités de protection des données qui est devenue une priorité dans un monde de plus en plus interdépendant. Ce thème touche au quotidien des fonctions des autorités de protection des données et à l'effectivité de leurs actions. La coopération entre autorités permet de profiter de synergies et d'apporter des réponses communes adéquates. Ainsi la conférence a fait le point sur différents modèles de coopération dans le monde, au sein de l'Union européenne ou du Conseil de l'Europe. Nous avons ainsi eu l'occasion de présenter le cadre légal de la coopération de la Convention 108. La Conférence a décidé la mise en place d'un groupe de travail chargé de faire des propositions en vue d'améliorer et de renforcer la coopération entre les autorités de protection des données des Parties à la Convention 108. Elle a également adopté une résolution relative à la révision de la Convention 108 appelant à préserver et, le cas échéant, à renforcer le niveau actuel de protection de la Convention comme proposé par le T-PD dans le texte adopté le 29 novembre 2012.

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

Pour la première fois en Afrique, la 36e Conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue du 13 au 17 octobre 2014 à l'Île Maurice. Elle réunissait des représentants de quelque 80 autorités nationales et régionales de protection des données, et des représentants des entreprises, des gouvernements, des organisations internationales et de la société civile, ainsi que des experts du monde académique. La Conférence comprenait comme à l'accoutumée deux parties: l'une réservée aux autorités de protection des données accréditées auprès de la conférence; l'autre ouverte aux parties intéressées. L'objectif est de permettre des échanges entre différents acteurs de la protection des données et de renforcer la coopération entre autorités et entre autorités et société civile. Lors de la session fermée, la conférence a débattu de l'Internet des objets qui, lié aux métadonnées, est l'un des grands défis auquel nos sociétés seront confrontées ces prochaines années et sur lequel un débat public devient urgent. La conférence a ainsi publié une déclaration rappelant les défis que pose l'internet des objets en termes de protection des données et de sécurité. La protection des données débute avec la collecte. Il est dès lors primordial de concevoir les technologies, les systèmes et les traitements en tenant compte dès le départ des exigences de la protection des données (privacy by design, privacy by default).

La partie ouverte de la conférence a permis d'aborder et d'échanger sur de nombreux sujets: les initiatives internationales en matière de coopération, la surveillance, la santé et le dossier électronique du patient, le cadre juridique de protection des données, notamment au sein de l'UE avec la question controversée du guichet unique, les évaluations des risques en matière de protection des données, les règles d'entreprises contraignantes dans le cadre des flux transfrontières de données et les enjeux du «big data» pour les droits et les libertés fondamentales.

Les commissaires ont en outre adopté:

- Une résolution sur la coopération internationale en matière de contrôle et d'enquête. L'objectif de cette résolution est de mettre en place un cadre mondial non-contraignant en matière de coopération transfrontière et de créer une plateforme sécurisée et neutre d'échanges d'informations pour les autorités accréditées à la conférence. Depuis l'adoption de la déclaration de Montreux, lors de la 27e conférence internationale, les commissaires à la protection des données élaborent des solutions pour renforcer la coopération entre eux afin d'améliorer l'application transfrontière des lois.

- Une résolution sur les mégadonnées appelant tous les acteurs du «big data» à respecter les principes de protection des données, notamment la limitation des finalités, le principe de proportionnalité, les obligations de transparence des traitements et la garantie des droits de personnes concernées (droit d'accès, information, droit de rectification ou d'effacement des données).

- Une résolution sur la protection de la vie privée à l'ère du numérique qui donne mandat au comité exécutif de la conférence internationale de participer à la discussion multipartite sur la protection du numérique sous l'égide des Nations Unies. Cette résolution appelle également à ce que les principes fondamentaux de protection des données, notamment énoncés dans la Convention 108 soient également respectés lors d'activités de surveillance électronique.

La 37e Conférence internationale des commissaires à la protection des données se déroulera à Amsterdam en automne 2015.

Association francophone des autorités de protection des données

En raison de l'épidémie d'Ebola en Afrique de l'ouest, l'Association francophone des autorités de protection des données (AFAPDP) a été contrainte d'annuler sa 8e conférence qui devait se dérouler à Ouagadougou (Burkina Faso). Elle a néanmoins tenu son Assemblée générale de manière électronique. Cette assemblée a permis de faire le point sur les activités de l'association durant l'année écoulée. En 2014, les autorités francophones de protection des données ont lancé deux outils pratiques: le premier est un Guide pratique pour la consolidation de l'état civil, les listes électorales et la protection des données rédigé en coopération avec l'Organisation internationale de la francophonie. Le second est constitué par des règles contraignantes d'entreprises destinées aux multinationales actives dans les pays francophones adoptées en 2013 (voir notre 21e rapport d'activités 2013 /2014, ch. 1.10.1) qui ont fait l'objet de plusieurs actions et notamment d'une formation des membres de l'AFAPDP en juillet 2014. Ces outils sont à la disposition des acteurs publics et des entreprises. Lors de cette Assemblée générale, l'AFAPDP a également adopté une résolution sur l'accompagnement des entreprises et de leurs efforts d'innovation technologique. Face à la collecte de plus en plus généralisée et massive de données, l'AFAPDP rappelle le rôle des autorités de protection des données, à savoir conseiller, sensibiliser et contrôler le respect des dispositions légales. Elle relève la disponibilité de ces autorités pour échanger avec les entreprises et les conseiller sur la manière d'être en conformité avec le droit à la protection des données. Enfin l'AFAPDP a adopté une déclaration à l'attention du XVe Sommet de la Francophonie à Dakar, dans laquelle elle encourage les États et gouvernements

francophones à soutenir la mise en place d'autorités indépendantes et de réseaux nationaux et internationaux de coopération dans le domaine de la protection des données et à adhérer aux instruments internationaux de protection des données, telle que la Convention 108.

Les autorités francophones tiendront leur prochaine conférence en juin 2015 à Bruxelles.

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

Le groupe de travail sur la sécurité de l'information et la protection de la sphère privée de l'Organisation de Coopération et de Développement Économiques (OCDE) a consacré ses travaux, cette année également, à la révision des lignes directrices de l'OCDE sur la sécurité de l'information.

La structure de ces lignes directrices a été améliorée et différentes définitions des thématiques ont été précisées. Sensibilisation, transparence et définition des risques possibles demeurent au cœur des travaux de révision. Il est intéressant de noter que concepts de protection de la sphère privée «privacy by design» et «privacy by default» sont dorénavant pris en compte dans ces travaux. Un rapport a été élaboré en parallèle qui explique et met en lumière la révision des lignes directrices.

L'importance des risques liés à l'Internet des objets et les dangers qu'il comporte pour la protection des données et la sécurité ont été reconnus et un rapport à ce sujet doit être élaboré d'ici la fin 2015. Outre la description des risques potentiels, ce rapport a pour objectif d'informer les utilisateurs sur les possibilités de protection. La lutte contre les risques sera déterminante pour le développement de l'économie dite «data driven» (guidée par les données).

L'établissement de la confiance dans l'économie data driven et l'importance accordée au traitement des données personnelles sont dépendants de la croissance économique du futur. La protection de la sphère privée y occupera une place essentielle, en particulier le rôle de l'utilisateur (consommateur) qui transmet, fournit ou génère sans en avoir conscience la plus grande partie des données personnelles disponibles en ligne. Des efforts seront entrepris notamment pour améliorer la transparence et renforcer la protection des données. Dans l'un de ses documents, l'OCDE montre les problèmes auxquels la sphère privée est confrontée dans ce contexte et comment les risques peuvent être abordés concrètement. Différentes approches ayant pour but la garantie des droits des utilisateurs sont actuellement soumises à la discussion. Il faut en outre renforcer la transparence des traitements de données, informer les consommateurs et respecter les principes de protection des données déjà applicables.

La révision des lignes directrices sur la protection des infrastructures d'information critiques a également été entamée. Dans ce contexte, une étude sur l'Internet des objets dans le contexte industriel a été présentée. Elle décrit les risques que l'Internet des objets présente pour les infrastructures étatiques (approvisionnement en eau et en énergie, approvisionnement de base, etc.). Les risques ne sont pas nouveaux, mais acquièrent une nouvelle dimension du fait des possibilités de connexion sur Internet. Cette étude ne traite pas des applications de l'Internet des objets, mais aborde uniquement les risques inhérents à l'interconnexion des infrastructures industrielles par Internet.

Conscient du fait qu'il est important de traiter de manière adéquate la gestion des risques dans le domaine de la protection des données, le groupe de travail a examiné dans quelle mesure il pouvait avoir une influence dans ce domaine auprès des entreprises, mais aussi du législateur. Outre l'incorporation éventuelle de la gestion des risques dans la législation, il est nécessaire que les entreprises intègrent, sur la base de modèles analogues ou identiques, la gestion des risques dans les autres processus de contrôle de l'entreprise. Le Groupe de travail Article 29 de l'Union européenne sur la protection des données a également élaboré quelques documents sur la gestion des risques en matière de protection des données, notamment sur les conditions-cadre et la régulation. Un large consensus règne sur la nécessité de disposer de critères uniformes d'évaluation et d'un cadre juridique clair. Toutefois, la mise en œuvre et la réalisation de l'évaluation des risques n'iront pas sans une charge de travail supplémentaire, notamment dans le domaine de l'interopérabilité.

Coopération internationale – groupe de coordination de contrôle Eurodac et VIS

Cette année encore, nous avons participé aux travaux des groupes de coordination pour le contrôle d'Eurodac et de VIS.

Durant l'année sous revue, nous avons participé aux séances du groupe de coordination pour la surveillance d'Eurodac. Le groupe de coordination Eurodac a élaboré un questionnaire concernant l'ordonnance Eurodac révisée, qui s'applique au niveau national à partir de juillet 2015. L'objectif consiste à déterminer quelles mesures d'application ont été prises à l'échelle du pays. Avec la nouvelle ordonnance Eurodac, les autorités pénales obtiendront également un accès. Pour que les autorités pénales helvétiques aient également accès aux données Eurodac, la Suisse doit d'abord mener des négociations avec l'UE.

Nous avons également participé aux séances du groupe de coordination pour le contrôle du système d'information sur les visas VIS. Le groupe de coordination VIS a adopté trois questionnaires concernant les accès des autorités en général, les

accès des autorités pénales et l'exercice des droits des personnes concernées au niveau national. Nous avons envoyé les trois questionnaires au Secrétariat d'État aux migrations (SEM, anciennement Office fédéral des migrations – ODM) et transmis ses réponses à Bruxelles. Parallèlement, nous avons participé au sous-groupe de travail qui analyse les questions juridiques soulevées en relation avec les prestataires de services externes, auxquels les consulats ont de plus en plus recours.

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. Il 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 du sous-groupe.

Le sous-groupe de travail s'est en particulier penché sur l'arrêt de justice de l'Union européenne concernant la conservation des données personnelles utilisées pour lutter contre le crime organisé et le terrorisme. 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 et d'un règlement portant sur la création d'un programme d'enregistrement des voyageurs.

Le sous-groupe de travail accompagne avec attention la création d'un cadre européen pour la communication des données PNR aux pays tiers et pour l'utilisation des données PNR à des fins répressives. Il observe également la révision du cadre juridique de protection des données de l'Union européenne instaurée par le Traité de Lisbonne.

Enfin, le sous-groupe de travail a élaboré une opinion sur le principe-clé de nécessité en matière de protection des données. Ce document a pour but de définir les concepts de nécessité et de proportionnalité que le législateur et les différentes autorités compétentes doivent prendre en compte dans le contexte du contrôle des frontières et de l'application de la loi.

Groupe de coordination du contrôle du SIS II

Le groupe de coordination du contrôle du SIS II (SIS II SCG) s'est réuni à deux reprises en 2014. Suite à une enquête relative à l'exercice du droit d'accès dans les différents États Schengen, le SIS II SCG a adopté un rapport qui sera publié prochainement. Il

en ressort notamment que le mécanisme de coopération entre autorités de protection des données doit être amélioré et qu'il convient de coopérer plus activement avec les organisations non gouvernementales et les autres acteurs de ce domaine afin d'encore mieux sensibiliser les personnes concernées à leurs droits.

Dans ce contexte, le groupe envisage également de créer un document permettant de mettre en place une approche commune pour élaborer les statistiques. Le groupe a mis à jour un guide sur les droits des personnes concernées qui a été publié en anglais et qui sera traduit prochainement dans diverses langues européennes.

À notre demande, le SIS II SCG s'est entretenu de la pratique de certaines autorités cantonales de police consistant à systématiquement comparer les fiches d'hôtel avec les signalements du SIS II et a émis un avis sur l'interprétation de l'article 45 de la convention d'application qui régit l'obligation de s'enregistrer dans les lieux d'hébergement et la mise à disposition des fiches de déclaration aux autorités compétentes. Il est arrivé à la conclusion qu'une vérification automatique et systématique de tous les signalements du SIS II avec les fiches de déclaration n'est pas conforme à la convention d'application. Le groupe a également préparé un questionnaire concernant l'accès au SIS II qui a été distribué aux autorités compétentes. Enfin, le groupe a décidé de créer un nouveau site internet du SIS II SCG.

Au niveau suisse, la coordination des activités liées à Schengen se fait au sein d'un groupe de coordination rassemblant le PFPDT et les autorités cantonales de protection des données. Ce groupe se réunit au minimum deux fois par année. Il permet aux autorités représentées de s'informer sur les développements en cours et sur les activités du SIS II SCG, de planifier des activités de contrôle et d'échanger des informations.

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

La 26e réunion du groupe de travail européen sur le traitement de cas relevant de la protection des données («Case Handling Workshop»), s'est tenu à Skopje du 6 au 7 octobre 2014. Le groupe de travail, constitué de représentants de 29 autorités nationales de protection des données s'est concentré sur plusieurs sujets sensibles actuels.

Le groupe a premièrement abordé la problématique de la collecte excessive des données personnelles et de la pesée des intérêts entre la protection des données et le droit d'accéder aux documents de l'administration publique. Dans un deuxième temps, la discussion a porté sur la vidéosurveillance et l'utilisation de données biométriques, deux sujets qui prennent de plus en plus d'ampleur. L'arrêt du 13 mai 2014 de la Cour de justice de l'Union européenne au sujet du droit à l'oubli a

longuement été discuté. Enfin, la discussion a porté sur les nouveaux défis soulevés par l'utilisation du WiFi ou des systèmes de suivi par Bluetooth. Il en ressort qu'il faut impérativement sensibiliser le public aux dangers de ces nouvelles pratiques et de les responsabiliser.

Tous les sujets thématisés ont été illustrés à l'aide de divers cas concrets tirés de la pratique des différentes autorités de protection des données. L'autorité de protection des données de l'Ancienne République Yougoslave de Macédoine publiera prochainement un manuel sur tous les sujets abordés lors de cette réunion.

2. Principe de la transparence

2.1 Demandes d'accès

Selon les chiffres qui nous ont été communiqués, 582 demandes d'accès ont été soumises aux autorités fédérales en 2014. Depuis l'entrée en vigueur de la loi sur la transparence en 2006, l'Administration fédérale n'avait encore jamais reçu autant de demandes. Les autorités ont accordé dans 297 cas un accès complet et dans 124 autres cas un accès partiel aux demandeurs. En revanche, la demande de consultation a été entièrement rejetée pour 122 demandes. Par ailleurs, 15 demandes d'accès ont été retirées et 17 cas étaient encore en suspens à la fin de l'année 2014.

2.1.1 Départements et offices fédéraux

En ce qui concerne le nombre de demandes d'accès (au total 575) et la pratique des autorités à cet égard, les chiffres sont globalement stables par rapport à l'année précédente. Ces données permettent de supposer que la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans) s'est imposée comme un instrument utile et efficace pour permettre aux particuliers et aux correspondants des médias d'obtenir des informations. Il n'en reste pas moins que l'on peut espérer que la loi sur la transparence continuera à être mieux connue et utilisée à l'avenir.

Selon les chiffres qui nous ont été fournis, l'office ayant reçu le plus de demandes d'accès (33) en 2014 est l'Office fédéral des migrations (ODM, depuis le 1er janvier 2015 Secrétariat d'État aux migrations SEM). Il est suivi par l'OFSP (32), l'OFEV (31), le CDF (28) et l'OFAG (25 demandes). Dans le peloton de tête des départements figurent le DETEC (106 demandes), le DFAE (101) et le DFI (95). Les chiffres du DFAE témoignent à nouveau d'une grande ouverture à la transparence avec 87 réponses entièrement positives sur 101 demandes au total, un accès partiel accordé dans un cas et seulement 8 refus complets. Sur 71 autorités, 16 nous ont annoncé qu'aucune demande ne leur avait été soumise pendant l'année sous revue. Le Préposé lui-même s'est vu confronté à 9 demandes en 2014, et a autorisé 8 accès complets et un partiel.

En ce qui concerne la perception d'émoluments liés à l'accès à des documents officiels, le montant total des frais facturés en 2014 (2600 CHF) s'est avéré étonnamment modeste. Si l'on tient compte du fait que ce montant ne correspond qu'à 9 des 575 demandes d'accès annoncées au total, dont 1000 CHF correspondent à une seule demande, les émoluments facturés paraissent négligeables. Une vue d'ensemble des émoluments perçus pour l'accès aux documents officiels depuis

l'entrée en vigueur de la loi sur la transparence en 2006 montre par ailleurs que moins de 3% de toutes les demandes annoncées au Préposé ont donné lieu à la perception d'émoluments. Au vu de ces chiffres, le Préposé ne comprend pas que l'administration veuille maintenir les dispositions et directives en vigueur de la Conférence des secrétaires généraux, puisque 97% de toutes les demandes ne donnent pas lieu à perception d'émoluments et que de nombreuses unités administratives se déclarent prêtes, dans le cadre de l'évaluation de la loi sur la transparence, à continuer à ne pas exiger d'émoluments à l'avenir (cf. notre présent rapport d'activités, ch. 2.4.1). C'est pourquoi le Préposé juge pertinent et nécessaire de réviser les règles concernant les émoluments pour les adapter à la pratique de l'administration. Il estime qu'il conviendrait ici soit d'augmenter sensiblement le montant exempté d'émoluments (p. ex. de 100 à 750 CHF) soit de prévoir directement la gratuité de l'accès aux documents officiels.

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 sur une base volontaire ne sont donc que partiellement pertinentes. Selon ces données, le temps de travail annoncé a encore diminué d'environ 20% malgré une progression du nombre de demandes (2010: 815 heures; 2011: 1519 heures; 2012: 2155 heures; 2013: 1707 heures; 2014: 1642 heures). En revanche, le temps de travail investi dans la participation à des procédures de médiation a progressé d'environ 85%, passant de 778 heures en 2013 à 1436 heures en 2014.

2.1.2 Services parlementaires

Les services parlementaires ont annoncé une seule demande d'accès en 2014. Dans le cas en question, l'accès aux documents a été entièrement rejeté.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a annoncé 6 demandes d'accès pour 2014, qui ont donné lieu à 5 accès complets et à un refus complet.

2.1.4 Demandes en médiation

En 2014, 90 demandes en médiation ont été soumises au total, soit une nette progression de plus de 18% (76 demandes en 2013). Contrairement à l'année précédente, la plupart des demandes déposées en 2014 provenaient de correspondants médias (44), suivis par les particuliers (19).

On peut déduire de ces chiffres les conclusions et remarques suivantes:

dans 246 cas, l'Administration fédérale a refusé l'accès de manière totale (122) ou partielle (124). Ces données sont à mettre en regard avec les 90 demandes en médiation qui nous sont parvenues. Pendant l'année sous revue, une demande en médiation a donc été soumise dans plus de 36% des cas de demandes d'accès totalement ou partiellement rejetées.

Au total, 85 demandes en médiation ont pu être liquidées en 2014, dont 35 qui avaient été soumises pendant cette même année, 25 dataient de 2013 et 25 de 2012. Dans 15 cas, une solution consensuelle a pu être trouvée entre les parties, 9 ayant permis de parvenir à une médiation au sens propre et les 6 procédures restantes ayant été menées à terme suite à une intervention du Préposé. Dans 2 cas, l'accès a été autorisé après ouverture de la procédure de médiation. Le Préposé a émis 49 recommandations là où aucune solution amiable n'était possible ou évidente de prime abord. Ces 49 recommandations ont permis de liquider 55 demandes en médiation. Par ailleurs, une demande en médiation a été retirée et une autre classée du fait de l'absence du demandeur lors de la négociation. Dans 7 cas, les conditions d'application de la LTrans n'étaient pas remplies. Dans 4 autres, la demande en médiation n'avait pas été soumise dans les délais.

Pendant l'année sous revue, le nombre de procédures de médiation menées à terme a atteint un record, ce qui s'explique notamment par le fait que le Préposé a pu, pour la première fois, engager deux stagiaires. Mais du fait d'importants retards dans le traitement des procédures en cours, les demandeurs doivent encore attendre plus longtemps que les 30 jours prévus par la loi avant que la procédure de médiation ne soit engagée.

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

2.2 Consultations des offices et autres prises de position

2.2.1 Introduction du nouveau standard de l'OCDE sur l'échange automatique de renseignements en matière fiscale

Le Préposé s'est exprimé dans le cadre de consultations des offices concernant l'ouverture de la procédure de consultation sur des projets d'échange international de renseignements en matière fiscale. À cet égard, il a pris position concernant les nouvelles dispositions de la loi sur l'assistance administrative fiscale et le projet de loi fédérale sur l'échange international automatique de renseignements en matière fiscale.

Les deux projets de loi contenaient chacun une disposition au contenu identique intitulée «Obligation de garder le secret». Le Préposé a souligné à ce sujet que cette disposition ne reflétait que l'obligation de garder le secret établie par la loi sur le personnel de la Confédération (Secret professionnel, secret d'affaires et secret de fonction) pour le personnel de la Confédération et a rappelé que la portée du secret de fonction avait été indirectement redéfinie avec l'entrée en vigueur de la loi sur la transparence (LTrans). Ne restent soumises au secret de fonction plus que les informations n'entrant pas dans le champ d'application de la LTrans, déclarées secrètes par des dispositions légales spéciales ou relevant de l'une des dispositions d'exception prévues dans la LTrans elle-même. Par conséquent, la disposition proposée concrètement ne permet pas de déduire qu'il y aurait des obligations plus étendues de maintenir le secret.

La possibilité d'accorder un droit de consultation dans le cadre d'une demande d'accès à des documents officiels dépend donc uniquement des dispositions de la loi sur la transparence (notamment art. 3 ss LTrans). Ainsi, les clauses d'exception prévues (par exemple le secret d'affaires ou les intérêts de la politique économique, financière et monétaire de la Suisse) ainsi que les dispositions relatives à la protection des données personnelles offrent suffisamment de possibilités pour refuser, limiter ou reporter l'accès à des documents officiels présentant un besoin de protection justifié.

De même, dans le domaine de l'échange international de renseignements en matière fiscale et de son application nationale, les dispositions d'exception existantes de la loi sur la transparence permettent de tenir dûment compte des circonstances concrètes dans le cas d'informations sensibles. Le Préposé a donc demandé au moins la suppression pure et simple de la dernière phrase du paragraphe, selon laquelle la consultation des dossiers officiels devait être refusée.

Les deux projets prévoyaient également des dispositions au contenu identique pour la publication de statistiques en vue de l'examen par les pairs du Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales. Selon ces dispositions, il ne devait exister aucun droit d'accès à des informations plus étendues que celles publiées dans les statistiques. Là encore, le Préposé demande que l'exclusion du droit d'accès soit simplement supprimée. Pour cela, il a renvoyé au champ d'application de la LTrans, qui ne s'applique pas à la procédure internationale d'entraide judiciaire et administrative, ainsi que sur ses clauses d'exception et sur les dispositions relatives à la protection des données personnelles et au secret statistique.

2.2.2 Projet de révision partielle de la loi sur l'aviation

Le Préposé a rejeté le projet de nouvelle disposition dans la loi sur l'aviation selon laquelle les documents concernant les activités de surveillance de l'Office fédéral de l'aviation civile devraient être soustraits à la loi sur la transparence.

Le Préposé s'est prononcé dans le cadre de la consultation des offices relative à l'ouverture de la procédure de consultation sur le projet de révision partielle 1+ de la loi sur l'aviation (LA). Le projet prévoyait au premier alinéa un devoir d'information active selon lequel l'Office fédérale de l'aviation civile (OFAC) informerait périodiquement le public sur son activité de surveillance. Pour le Préposé, cet alinéa n'est pas suffisamment concret car il ne précise pas les contenus de l'activité de surveillance sur lesquels l'OFAC donnerait des informations, ni ne définit plus précisément ce que recouvre la notion «périodiquement». Indépendamment d'un éventuel devoir actif d'information, il existe du reste toujours la possibilité de déposer une demande d'accès conformément à la loi sur la transparence (LTrans).

Le second alinéa prévoyait de retirer du champ d'application de la LTrans les rapports d'inspection et d'audit de l'OFAC ainsi que tous les documents livrant des conclusions sur résultats et les informations rassemblés au cours de ces contrôles.

Le préposé a rejeté la réglementation ici proposée. Il a souligné que les instruments juridiques de la LTrans, avec toutes ses dérogations, suffisaient pour tenir équitablement compte du besoin de protection des informations sensibles. En outre, cette loi repose sur la notion de document officiel et ne prévoit pas d'exclure des catégories individuelles de documents comme les rapports d'inspection ou d'audit.

Par ailleurs, le Préposé a réfuté l'argumentation de l'OFAC selon laquelle les rapports ne seraient plus formulés avec suffisamment de précision et de pertinence s'ils n'étaient pas traités de manière confidentielle. Il estime que le devoir légal de surveillance de l'OFAC ainsi que les obligations de collaboration des entreprises surveillées ne sont pas entravés par la LTrans. Afin d'étayer sa position, le préposé a cité

le Contrôle fédéral des finances (CDF), qui œuvre également dans des domaines de contrôles sensibles et conclut aujourd'hui, au terme de sept ans d'expérience de la LTrans, que la qualité de son travail n'était pas entravée par cette loi.

Le préposé a considéré l'argumentation, selon laquelle les rapports contenaient souvent des détails techniques difficiles à mettre en perspective par le public, comme arrogante et indéfendable. Au plus tard depuis l'entrée en vigueur de la LTrans, il n'appartient plus à l'administration de juger si certaines informations sont compréhensibles par le grand public ou si une personne précise est à même de tirer de «justes» conclusions d'un document. Il estime que cela équivaudrait à une mise sous tutelle du citoyen et a rappelé que le caractère compréhensible d'une information n'était pas l'un des critères prévus par la LTrans.

Le Préposé a par ailleurs souligné que telle qu'elle est formulée, la disposition prévue permettrait de retirer du champ d'application de la LTrans l'ensemble de l'activité de surveillance de l'OFAC, ce qui ne se justifie pas étant donné l'intérêt public légitime à ce que cette activité de surveillance soit correctement accomplie dans le domaine de l'aviation.

Enfin, le Préposé a fait remarquer qu'en adoptant la LTrans, le législateur a donné un signal clair contre les domaines et documents secrets dans l'administration fédérale, signal qui en définitive doit aussi valoir pour les autorités de surveillance tenues, de par la loi, de contrôler d'autres unités administratives ou des particuliers. On ne voit donc pas pourquoi des autorités elles-mêmes chargées de tâches d'audit et d'inspection entendent se soustraire à tout contrôle basé sur la LTrans alors que le Tribunal administratif fédéral lui-même a reconnu un intérêt public à la traçabilité de l'activité de surveillance d'une autorité (A-2434/2013 du 9 décembre 2013, consid. 10.2).

2.2.3 Révision de la loi fédérale et de l'ordonnance sur les marchés publics

Dans le cadre de la procédure de consultation, le Préposé a pris position sur les projets de révision de la loi fédérale sur les marchés publics (LMP) et de l'ordonnance sur les marchés publics (OMP).

Le Préposé salue l'orientation générale de la révision de la LMP et de l'OMP, visant notamment à renforcer la transparence des marchés publics ainsi qu'à favoriser une utilisation efficiente des fonds publics, à encourager la concurrence et enfin à lutter contre la corruption. Le Préposé a estimé important que l'amélioration de la transparence en matière de droit des marchés publics ne soit pas seulement un objectif parmi d'autres mais qu'il constitue un instrument efficace, en quelque sorte le moteur permettant d'atteindre les autres objectifs visés par la présente révision.

En revanche, il a regretté que cette révision n'ait pas été l'occasion de se pencher aussi, dans le cadre des objectifs de transparence, sur l'activité d'information réalisée sur demande par les autorités (information passive) et d'assurer ainsi la coordination entre la LMP et la loi fédérale sur le principe de la transparence dans l'administration (LTrans). Il a notamment déploré l'absence d'une mention indiquant qu'outre les différentes dispositions relatives à l'information d'office des autorités (information active), le droit d'accès à des documents officiels des marchés publics s'applique sur la base de LTrans.

Dans ce contexte, le Préposé a souligné que la liste «non-publique» des soumissionnaires sanctionnés prévue à l'art. 47 al. 4 de l'avant-projet devait être rendue accessible, au moins sur demande, conformément aux dispositions de la loi sur la transparence. Au vu du changement de paradigme introduit par la LTrans, le caractère «non-public» de cette liste peut uniquement être compris dans le sens que celle-ci n'a pas à être publiée de manière active. En revanche, une disposition prévoyant la «non-publicité» de cette liste ne constitue pas pour autant une disposition spéciale au sens de l'art. 4 LTrans, ce qui en exclurait d'emblée l'accessibilité en se basant sur la loi sur la transparence. Bien plus, il convient de vérifier dans chaque cas si l'accès doit être refusé ou limité en raison de l'application d'une exception figurant dans la LTrans.

Par ailleurs, le Préposé a jugé trop partielle et focalisée l'indication figurant dans le rapport explicatif selon laquelle une trop grande transparence favoriserait des pratiques concertées et pourrait se révéler anticoncurrentielle. Il estime en effet au contraire que le manque de transparence en matière de marchés publics peut être une source de corruption et de mauvaise gestion, comme cela a déjà été clairement démontré dans la pratique.

2.2.4 Consultation des offices relative à la révision de l'art. 15 de l'Ordonnance sur la transparence

Suite à l'arrêt du Tribunal fédéral 1C_550/2013 concernant la réduction des émoluments applicable aux correspondants des médias, la Conférence des secrétaires généraux (CSG) a chargé le groupe de travail interdépartemental Protection des données, sous la direction de la Chancellerie fédérale (ChF), d'examiner la jurisprudence du Tribunal fédéral et la préparation d'une révision de l'ordonnance sur le principe de la transparence dans l'administration (OTrans). Après des discussions avec un sous-groupe de ce groupe de travail, l'OFJ a soumis, en tant qu'autorité compétente pour la législation en matière de transparence, un projet de révision de l'art. 15 OTrans concernant les émoluments.

Dans le cadre de sa participation à ce sous-groupe et de la procédure de consultation des offices sur le projet de révision des émoluments, le Préposé a pris position

sur plusieurs points. Il a d'abord estimé qu'une base légale formelle était nécessaire pour modifier le droit des émoluments. Il a ensuite indiqué que la loi sur la transparence prévoyait un droit et non une obligation de percevoir des émoluments. Enfin, le Préposé a souligné que la norme prévue ne tenait pas compte de la jurisprudence du Tribunal fédéral puisque selon cette dernière, les émoluments pouvaient aussi être librement réduits de plus de de 50% pour les correspondants des médias. L'OFJ a partiellement repris les propositions de modification du Préposé.

Le nouvel art. 15, al. 4, OTrans est en vigueur depuis le 1er septembre 2014. Il prévoit, pour la perception des émoluments, une réduction d'au moins 50% pour les correspondants des médias, avec la possibilité de renoncer à cette réduction pour les demandes d'accès nécessitant un surcroît important de travail (concernant les émoluments, voir également notre 21e rapport d'activités 2013/2014, ch. 2.6.1).

2.3 Varia

2.3.1 Évaluation de la loi sur la transparence et participation au groupe d'accompagnement

En 2014, la loi sur la transparence a fait l'objet d'une évaluation pour la seconde fois depuis son entrée en vigueur. Le Préposé a également pris part au groupe d'accompagnement. Le rapport final ne présente pas de résultats très différents de ceux de la première évaluation, mais fournit des informations et commentaires intéressants.

La loi sur la transparence (LTrans) a fait l'objet d'une première évaluation en 2009 (cf. www.leprepose.ch ¬– Principe de la transparence – Évaluation). Après le récent regain de critiques de la part des autorités concernant l'application de la LTrans, la Conférence des secrétaires généraux a demandé une nouvelle évaluation de son exécution et de son efficacité. L'évaluation de la LTrans a été confiée à l'Office fédéral de la justice (OFJ), qui a constitué un groupe d'accompagnement, composé des conseillers à la transparence des départements et de la Chancellerie, d'une représentation des Archives fédérales et du Préposé. L'entreprise Büro Vatter AG mandatée pour l'évaluation a remis son rapport final à l'OFJ fin 2014. Le Conseil fédéral a pris connaissance de ce rapport au printemps 2015 et a, sur la base des résultats de l'évaluation, chargé le DFJP de procéder à une révision partielle de la LTrans.

Dans le cadre de l'évaluation, les conseillers à la transparence des départements et de la Chancellerie et douze conseillers à la transparence d'autorités choisies ont été interrogés, ainsi que des demandeurs, des experts des médias et le Préposé.

Les conclusions auxquelles sont parvenus les évaluateurs n'ont pas surpris le Préposé, car elles coïncident largement avec celles de l'évaluation de 2009:

- Changement de paradigme: le changement de paradigme régulièrement demandé depuis l'entrée en vigueur de la LTrans n'a toujours pas été mis en œuvre dans l'ensemble de l'administration fédérale. Les demandeurs ont encore souvent l'impression que certaines autorités s'opposent à l'exécution de la LTrans.
- Documents disponibles: comme il y a six ans, la nouvelle évaluation est parvenue à la conclusion selon laquelle il est difficile pour les personnes intéressées d'être informées des documents qui sont disponibles au sein de l'administration fédérale.
- Coordination entre et au sein des départements: les deux évaluations témoignent de pratiques divergentes dans le traitement des demandes d'accès par-delà les autorités et les départements, et proposent donc d'exploiter des synergies hors des limites des unités administratives et de créer un groupe de travail pour l'échange d'expériences.

- Pratiques en matière d'émoluments: les experts de l'évaluation de 2014 constatent eux aussi un manque d'uniformité dans la perception d'émoluments au sein de l'administration, et proposent également d'augmenter le montant de l'exonération.
- Augmentation des ressources en personnel du Préposé: tous les groupes interrogés dans le cadre de la seconde évaluation (autorités fédérales, conseillers à la transparence des départements, experts des médias, demandeurs) ont préconisé que le Conseil fédéral apporte les ressources requises pour réduire la durée de la procédure de médiation. L'évaluation de 2009 était déjà parvenue à cette conclusion. Cependant, le Conseil fédéral a rejeté à ce jour toutes les demandes de ressources du Préposé.

Le rapport final contient pour le Préposé certaines informations notables sur ces conclusions. Quelques unités administratives ont encore du mal à se faire à ce changement de paradigme près de neuf ans après l'entrée en vigueur de la loi sur la transparence, comme le montre notamment le fait que l'on discute encore de savoir si les courriels ou les documents classifiés relèvent de la LTrans. Dans les entretiens avec les experts, il a été évoqué que les procès-verbaux de commissions extraparlementaires devaient être exclus du champ d'application de cette loi. Cela n'est guère étonnant dans la mesure où des tentatives ont déjà été entreprises dans le passé pour exclure totalement ces commissions (notamment la Commission de la concurrence) de la loi sur la transparence.

Les experts se sont attelés à la question des procès-verbaux et suggèrent un réexamen. Ils établissent une comparaison avec les commissions parlementaires, dont les délibérations sont confidentielles conformément à la loi sur le Parlement. Cette conclusion n'est pas concevable pour le Préposé: d'une part, la comparaison est faussée car les commissions extraparlementaires remplissent notamment des missions qui devraient normalement relever de l'administration; d'autre part, le Tribunal administratif fédéral a déjà jugé que les commissions extraparlementaires comme leurs procès-verbaux relevaient de la loi sur la transparence.

Le rapport final relève également la demande de quelques autorités de surveillance d'exclure leurs activités du champ d'application de la LTrans. Selon le Préposé, il n'est pas acceptable que des autorités de surveillance revendiquent le secret pour leur domaine d'activité bien qu'elles surveillent d'autres organes privés et publics dans l'intérêt général. À cet égard, on peut noter le volte-face positif opéré en 2014 par le Contrôle fédéral des finances (CDF) en ce qui concerne le principe de transparence. Dans son communiqué de presse du 23 juin 2014, cette instance, qui assume des fonctions de surveillance et de contrôle, dresse un bilan positif de la LTrans après sept années d'application, et estime ne pas être entravée dans son travail par ce texte.

La constatation figurant dans le rapport final, selon laquelle un changement à la tête d'une autorité a mené à l'application de la LTrans, est également intéressante. Elle n'étonne pas le Préposé, qui estime depuis longtemps déjà que la position de la direction d'une autorité exerce une influence déterminante sur la manière dont est appliqué le principe de transparence. Par ailleurs, le Préposé constate régulièrement que la volonté d'appliquer la LTrans dépend fortement des personnes impliquées. On peut supposer qu'il existe également dans d'autres départements des services (p. ex. secrétariats généraux et offices fédéraux, mais aussi certaines directions de divisions ou de sections, ou certains services de communication) qui ne recherchent pas, du moins directement, à appliquer le principe de transparence exigée par le législateur. Un soutien clair du principe de transparence à tous les échelons de direction de l'administration fédérale serait souhaitable.

Le rapport d'évaluation a notamment analysé 106 procédures de médiation. Il s'avère notamment que 90% des procédures de médiation menées par le Préposé n'ont pas entraîné de procédure judiciaire. Ainsi, l'objectif formulé dans le Message relatif à la loi sur la transparence (FF 2003 2018), à savoir le fait d'éviter des procédures administratives et judiciaires en créant une procédure de médiation, a pu être atteint.

Parallèlement, une comparaison des recommandations du Préposé avec les jugements rendus a été réalisée dans le cadre de l'évaluation. L'analyse juridique des arrêts pertinents du Tribunal administratif fédéral et du Tribunal fédéral a montré que les recommandations du Préposé étaient suivies par les tribunaux et qu'aucun jugement exécutoire s'écartant notablement de ces recommandations n'avait été rendu. Il arrive même parfois que le Tribunal administratif fédéral renvoie expressément aux recommandations du Préposé. Dans ce contexte, il n'est guère étonnant que les évaluateurs constatent dans leur rapport une bonne acceptation des recommandations, en particulier par les demandeurs. Et ce, même lorsque les recommandations du Préposé sont en leur défaveur.

En outre, tous les demandeurs interrogés s'accordent à penser qu'une procédure de médiation gratuite doit être possible en cas de restriction d'accès par les autorités (91% d'opinions positives, 9% plutôt positives). Ils jugent les recommandations du Préposé extrêmement positives: 91% des demandeurs interrogés considèrent comme «positif», et 8% comme «plutôt positif», le fait que le Préposé motive ses recommandations. En d'autres termes, près de 100% des demandeurs apprécient particulièrement le niveau d'explications et les motivations détaillées des recommandations. Dans le même temps, sept demandeurs sur dix regrettent que les recommandations du Préposé n'aient pas d'effet juridique immédiat. Au vu de ces résultats, il n'est pas étonnant de constater que les demandeurs jugent le travail du Préposé particulièrement positif.

Certains experts des médias considèrent la procédure de médiation comme une institution utile. Les recommandations du Préposé rencontrent un bon niveau d'acceptation parmi eux, car elles représentent à leurs yeux des directives d'application de la loi sur la transparence dans le quotidien de l'administration. Le Préposé est même perçu dans une certaine mesure comme le «moteur» du principe de transparence. Pour d'autres experts, la procédure est trop lourde et trop compliquée. Il est ainsi notamment proposé de développer les compétences du Préposé – qui devrait pouvoir statuer directement plutôt qu'émettre des recommandations.

Les douze autorités interrogées estiment également dans leur grande majorité que la procédure de médiation permet d'éviter des procédures judiciaires. Ainsi, elles estiment pour deux tiers d'entre elles au moins que les recommandations du Préposé jouent un rôle, du moins partiel, dans la constitution de la pratique. Cependant, la plupart des autorités émettent un avis critique: deux d'entre elles estiment qu'il n'y pas besoin de procédures de médiation, car il s'agit uniquement de faire appliquer la loi sur la transparence et non de tenir compte de sensibilités. Certaines des autorités interrogées estiment que le Préposé accorde globalement trop de poids à la transparence, qu'il est «trop favorable à la transparence» et qu'il a tendance à être «plutôt opposé aux autorités».

La durée de la procédure de médiation est jugée par tous – y compris par le Préposé lui-même – insatisfaisante. Dans les faits, elle constitue une limitation de l'accès aux documents officiels et peut être utilisée abusivement par les autorités pour reporter l'accès aux documents souhaités dans l'espoir de voir la motivation du demandeur diminuer avec le temps. Il est intéressant de noter dans ce contexte que selon tous les groupes interrogés (y compris certaines voix de l'administration fédérale), le Conseil fédéral devrait enfin accorder au Préposé les ressources nécessaires pour une application efficace de la loi sur la transparence et pour réduire la durée de la procédure de médiation. Les experts pensent également que l'accélération de la procédure passe par l'augmentation des ressources du Préposé. Ils parviennent ainsi à la même conclusion que les évaluateurs de 2009, confirmant ainsi les demandes répétées de ressources adressées par le Préposé au Conseil fédéral, que ce dernier a toujours rejetées à ce jour.

En ce qui concerne la durée de la procédure de médiation, le Préposé a encore souligné qu'un délai de trente jours pour l'exécution d'une telle procédure était irréaliste et allait en fin de compte à l'encontre de toute logique. De par la nature même de la procédure de médiation, sa limitation dans le temps s'oppose à l'obtention d'un accord. Même avec une allocation de ressources suffisante, le respect d'un délai pour parvenir à une solution n'est pas possible dans les affaires les plus complexes. Dans la pratique, on constate régulièrement que la simple obtention d'un rendez-vous avec les parties prenantes peut poser des difficultés et qu'il peut être impossible d'arriver à une rencontre pendant un mois. Par conséquent, le Préposé

maintient sa demande de suppression de ce délai, parallèlement à la mise à disposition de ressources en personnel suffisantes.

En résumé, le Préposé estime que les conclusions de l'évaluation concernant la procédure de médiation sont satisfaisantes. La procédure s'est établie pendant les neuf années qui se sont écoulées depuis l'entrée en vigueur, et les parties prenantes la jugent de manière majoritairement positive. Les évaluateurs suggèrent de réduire la durée de la procédure de médiation (en augmentant les ressources du Préposé en personnel) tout en maintenant sa rigueur. En principe, ils sont favorables à une accélération sans pour autant que soit abandonné l'avantage essentiel de la procédure du point de vue des demandeurs, à savoir le niveau d'explication et les motivations détaillées des recommandations.

Il reste à espérer, en cas d'éventuelle accélération, que le Conseil fédéral tiendra également compte des intérêts des demandeurs notamment du maintien de la qualité des recommandations. Le Préposé suivra la suite des événements avec attention.

2.3.2 Relations avec les préposés cantonaux à la transparence – groupe de travail sur la médiation

Le Préposé ainsi que les préposés cantonaux à la transparence, qui mènent également des procédures de conciliation, se sont à nouveau rencontrés en 2014 pour un échange approfondi d'expériences. Il a ainsi été possible, dans le cadre du «Groupe d'intervision sur la gestion consensuelle des conflits en matière de transparence» mis sur pied à l'automne 2011, de débattre des questions relatives à l'activité de médiation et au principe de la transparence. Cette collaboration est non seulement importante mais aussi précieuse pour les acteurs impliqués, en particulier parce que la législation sur la transparence constitue un domaine du droit récent en Suisse. À la suite de mutations, le groupe de travail a connu l'année dernière un changement dans sa composition. Parallèlement, il a été décidé que les séances informelles seraient organisées en alternance par les différents membres et par conséquent que les séances se tiendraient également dans les cantons.

3. Le PFPDT

3.1 Neuvième Journée de la protection des données

Lors de la 9e Journée internationale de la protection des données, nous avons organisé une table ronde à la Maison des générations de Berne sur la problématique de la protection des données des applications de santé et des technologies portables (wearables). Nous avons pu constater le grand intérêt suscité par le sujet.

Les dernières innovations technologiques dans le domaine de la santé ouvrent de nouvelles possibilités à la recherche médicale et modifient durablement notre société. La tendance croissante à l'»automesure corporelle» (quantified self) fait progresser le volume des données de santé de manière exponentielle, et les intérêts commerciaux autour de ces informations sont nombreux. Par conséquent, le risque d'un accès non autorisé à des informations parfois très sensibles est en augmentation. Lors d'une table ronde réunissant des experts de la politique, de l'économie et de la recherche, Hanspeter Thür, Préposé fédéral à la protection des données et à la transparence, a pu éclairer divers aspects sous un jour critique et placer au centre des débats l'importance de la prise de conscience de la protection des données et de l'autodétermination en matière d'information.

Lors d'une discussion animée, les experts ont analysé sous un angle critique et diversifié le sujet de la protection des données autour des applications de santé et des technologies portables («wearables»). Bien que les représentants de la recherche et de l'économie soient globalement favorables à l'automesure numérique et y voient des avantages pour les patients, ils sont conscients du risque lié au traitement de données de santé. Hanspeter Thür a souligné que la protection des données devrait être prise en compte dès la phase de développement de nouvelles technologies (privacy by design) et exige des configurations propices à cette protection (privacy by default). Sur le plan politique, un renforcement de la loi sur la protection des données est donc à prévoir. Le Préposé estime que la Suisse doit demeurer exemplaire en matière de protection des données et ne pas perdre de terrain par rapport à l'Union européenne car cela aurait également des conséquences négatives pour l'économie helvétique.

La table ronde avec participation du public a permis de couvrir largement le sujet de la protection des données, de sorte que les domaines de la cybersanté (eHealth) et des mégadonnées (big data) ainsi que les aspects éthiques ont pu être abordés.

3.2 Publications du PFPDT au cours de l'année sous revue

Les citoyens intéressés peuvent trouver des informations complètes sur les thèmes actuels de la protection des données sur notre site Internet www.leprepose.ch. Pendant l'année sous revue, nous avons notamment publié des explications sur les mégadonnées, sur le droit à l'oubli, l'utilisation de drones, la protection des données et la recherche et les systèmes de contrôle d'accès aux centres de loisirs. Par ailleurs, nous avons publié une série de recommandations dans le domaine de la loi sur la transparence.

Les mégadonnées (Big Data) offrent de nouvelles chances de découvertes sociales ou scientifiques, ainsi que des opportunités d'utilisation commerciale pour les entreprises. Le big data peut constituer une menace pour la sphère privée si les données personnelles traitées ne sont pas, ou pas suffisamment, anonymisées. Pour la protection de la personnalité, nous demandons donc une configuration technique favorable à la protection des données (privacy by default). Celle-ci doit être prise en compte, et la sécurité des données garantie, dès la phase de conception (privacy by design). En outre, des exigences élevées doivent être appliquées aux mégadonnées en termes de transparence et de procédure (www.leprepose.ch, Protection des données – Internet et ordinateur – Big Data).

L'arrêt de la Cour de justice de l'Union européenne du 13 mai 2014 concernant le droit à l'oubli, qui rend les opérateurs de moteurs de recherche responsables du traitement des données personnelles effectué sur leurs sites web et exige qu'ils suppriment les liens vers ces pages sur demande et à certaines conditions, a également suscité des discussions en Suisse. Afin de tenir compte de l'évolution technologique et de la numérisation croissante, l'UE projette une révision de son cadre juridique. Chez nous aussi, des solutions efficaces doivent être trouvées pour mieux protéger la dignité des personnes concernées et le droit à la sphère privée sur Internet (www.leprepose.ch, Protection des données – Internet et ordinateur – Droit à l'oubli).

Grâce au progrès technologique, les drones sont devenus de plus en plus petits, légers, avantageux et faciles à manoeuvrer. Ils sont donc de plus en plus utilisés, à des fins privées ou commerciales. Comme les drones ont en général une caméra embarquée, ils peuvent être utilisés pour la vidéosurveillance. Les personnes aux commandes de drones doivent donc respecter les dispositions sur la protection des données dès que les prises de vues contiennent des personnes identifiées ou identifiables. Sur notre site Internet, nous décrivons clairement et en détail ce qu'il convient de savoir concernant l'utilisation de drones (www.leprepose.ch, protection des données – technologies – vidéosurveillance – drones).

De même, on recourt de plus en plus aux systèmes de localisation de personnes, par exemple pour optimiser les flux de trafic ou de personnes, ou pour analyser le comportement des clients, notamment à des fins de marketing. Ces systèmes permettent même, dans certains cas, de recueillir des données sensibles ou d'établir des profils de la personnalité. C'est pourquoi il convient de faire preuve de prudence lors de leur utilisation. Notre site Internet indique les principaux aspects de la protection des données auxquels il faut veiller dans le cadre de l'utilisation de tels systèmes de localisation (www.leprepose.ch, protection des données – technologies – localisation de personnes).

Les chercheurs sont responsables des données personnelles qu'ils traitent. Dans le cas des informations collectées pour la recherche médicale, leur traitement est soumis au consentement préalable des personnes concernées ou à l'existence d'une base légale. Même si chaque cas individuel doit être considéré dans le contexte de la recherche en question et à la lumière de ses spécificités, les projets de recherche doivent si possible utiliser des données anonymisées. Le résultat de la recherche doit également être publié sous une forme anonyme (www.leprepose.ch, protection des données – statistique, registre et recherche – protection des données et recherche en général).

La recherche médicale requiert tout particulièrement des informations permettant d'identifier les personnes concernées, et répond le plus souvent à un intérêt public et/ou privé important. Les données personnelles ainsi traitées pouvant être sensibles, on comprend dès lors que certaines personnes hésitent à donner des informations sur leur santé à des tiers. (www.leprepose.ch, protection des données – statistique, registre et recherche – recherche médicale).

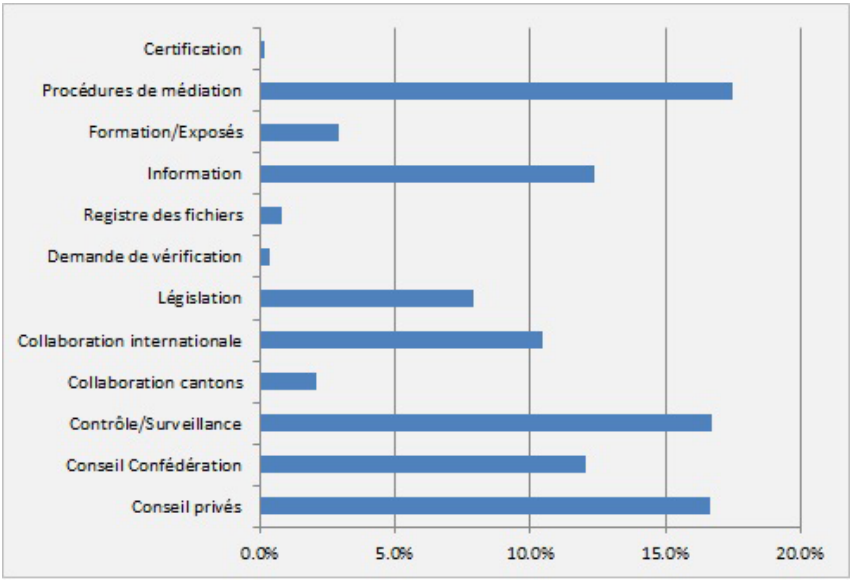
Pour les entreprises, permettre à leurs collaborateurs d'utiliser leurs propres appareils mobiles pour leur travail (bring your own device – BYOD) présente des avantages en termes de répartition des coûts, de joignabilité ou de connaissance des appareils, mais soulève également divers problèmes pour les deux parties du point de vue de la protection des données. D'une part, il existe un risque que l'employeur obtienne l'accès à des informations personnelles de l'employé si celles-ci ne sont pas clairement séparées de son activité professionnelle. D'autre part, des tiers non autorisés peuvent avoir ainsi accès à des données de l'entreprise si l'appareil est également utilisé dans le temps libre du collaborateur, par exemple par des membres de sa famille. Et le risque de perte ou de mauvaise utilisation des informations de l'entreprise peut également être renforcé par une utilisation privée (www.leprepose.ch, protection des données – secteur du travail – Bring Your Own Device).

Notre site Internet propose enfin un nouveau feuillet thématique sur l'exploitation des systèmes de contrôle d'accès, utilisés dans les stations de ski, mais aussi dans les clubs de tennis, les centres de fitness et autres prestataires de loisirs. Notre feuillet montre quelles informations peuvent être collectées, qui peut y avoir accès,

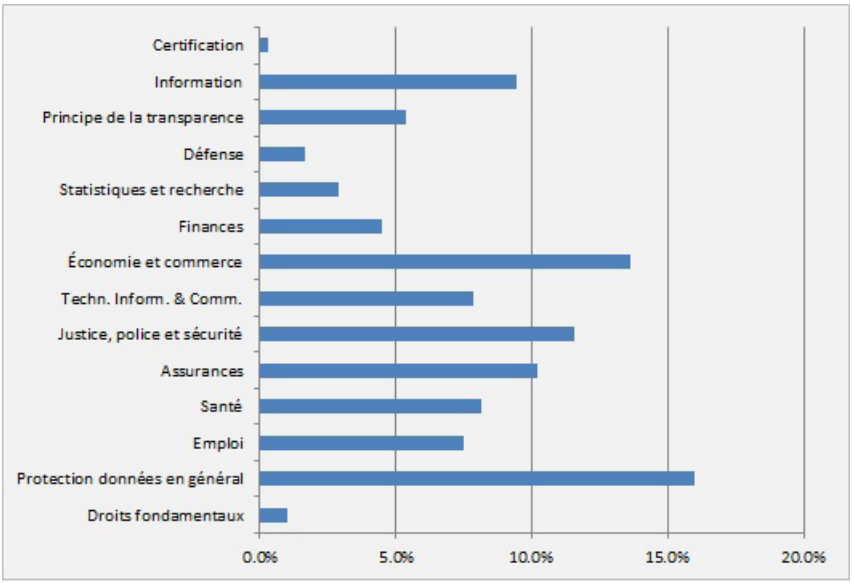
à quelles fins les données peuvent être utilisées, etc. (www.leprepose.ch – protection des données – documentation – feuillets thématiques – systèmes de contrôle d'accès dans les centres de loisirs).

3.3 Statistique des activités du PFPDT du 1er avril 2014 au 31 mars 2015

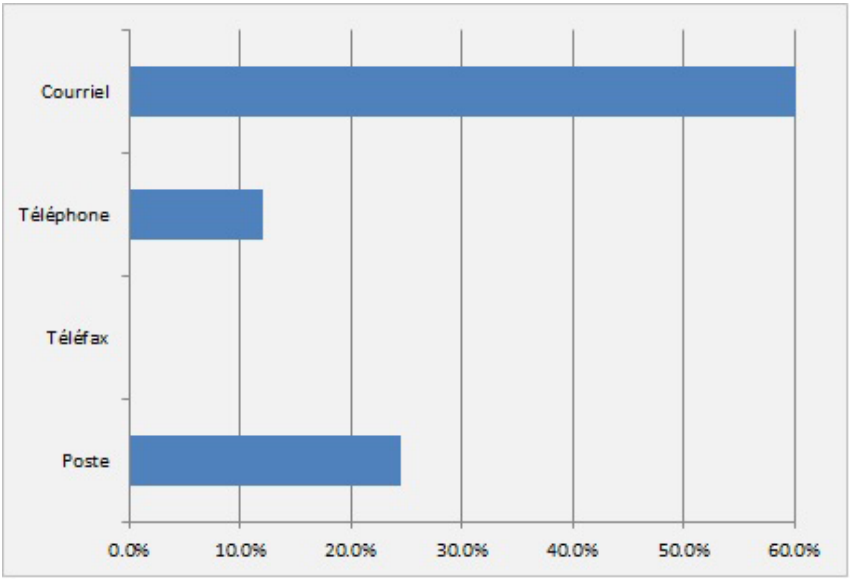
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.4 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014)

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
ChF	18	12	2	4	0	0
DFAE	101	87	8	6	0	0
DFI	95	31	22	30	10	2
DFJP	67	23	21	20	2	1
DDPS	33	8	13	11	1	0
DFF	71	41	12	16	0	2
DEFR	84	37	24	20	0	3
DETEC	106	58	20	17	4	7
Total 2014 (en %)	575 (100 %)	297 (51 %)	122 (21 %)	124 (22 %)	17 (3 %)	15 (3 %)
Total 2013 (en %)	469 (100 %)	218 (46 %)	122 (26 %)	103 (22 %)	8 (2 %)	18 (4 %)
Total 2012 (en %)	506 (100 %)	223 (44 %)	138 (27 %)	120 (24 %)	6 (1 %)	19 (4 %)
Total 2011 (en %)	466 (100 %)	203 (44 %)	126 (27 %)	128 (27 %)	9 (2 %)	-
Total 2010 (en %)	239 (100 %)	106 (45 %)	62 (26 %)	63 (26 %)	8 (3 %)	-
Total 2009 (en %)	232 (100 %)	124 (54 %)	68 (29 %)	40 (17 %)	-	-
Total 2008 (en %)	221 (100 %)	115 (52 %)	71 (32 %)	35 (16 %)	-	-

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
BK	9	4	2	3	0	0
PFPDT	9	8	0	1	0	0
Total	**18**	**12**	**2**	**4**	**0**	**0**

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	101	87	8	6	0	0
Total	**101**	**87**	**8**	**6**	**0**	**0**

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	14	4	4	5	0	1
BFEG	0	0	0	0	0	0
OFC	3	2	0	1	0	0
AFS	2	2	0	0	0	0
METEO CH	0	0	0	0	0	0
BN	0	0	0	0	0	0
OFSP	32	9	8	11	4	0
OFS	6	2	0	4	0	0
OFAS	10	5	2	2	1	0
OSAV	6	1	2	3	0	0
MNS	0	0	0	0	0	0
SWISS-MEDIC	21	5	6	4	5	1
SUVA	1	1	0	0	0	0
Total	**95**	**31**	**22**	**30**	**10**	**2**

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	7	2	1	2	2	0
OFJ	3	2	1	0	0	0
FEDPOL	8	3	2	3	0	0
METAS	2	1	0	1	0	0
ODM	33	9	14	10	0	0
ISDC	7	2	1	4	0	0
IPI	3	2	1	0	0	0
CFMJ	2	2	0	0	0	0
CAF	0	0	0	0	0	0
ASR	1	0	1	0	0	0
CSI	1	0	0	0	0	1
CNPT	0	0	0	0	0	0
Total	**67**	**23**	**21**	**20**	**2**	**1**

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	10	3	3	4	0	0
Défense/ armée	2	2	0	0	0	0
SRC	13	2	4	6	1	0
armasuisse	7	0	6	1	0	0
OFSPO	1	1	0	0	0	0
OFPP	0	0	0	0	0	0
Total	**33**	**8**	**13**	**11**	**1**	**0**

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	9	6	2	1	0	0
UPIC	3	1	0	2	0	0
AFF	0	0	0	0	0	0
OFPER	3	2	1	0	0	0
AFC	12	4	4	2	0	2
AFD	7	4	2	1	0	0
RFA	0	0	0	0	0	0
OFCL	3	2	0	1	0	0
OFIT	2	2	0	0	0	0
CDF	28	18	1	9	0	0
SFI	2	0	2	0	0	0
PUBLICA	0	0	0	0	0	0
CdC	2	2	0	0	0	0
Total	**71**	**41**	**12**	**16**	**0**	**0**

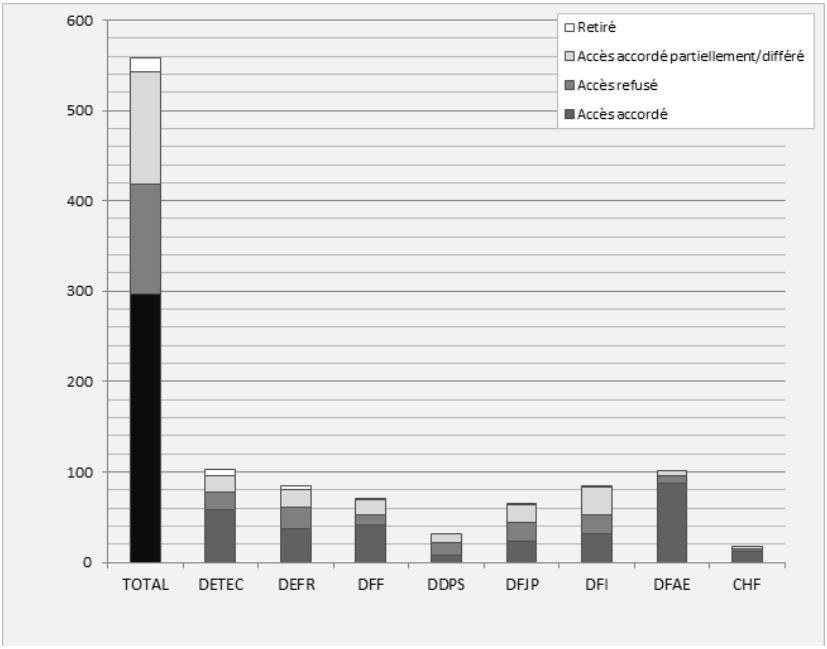
Département fédéral de l'économie, de la formation et de la recherche DEFR

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	2	1	1	0	0	0
SECO	20	4	12	4	0	0
SEFRI	8	4	3	1	0	0
OFAG	25	10	5	10	0	0
OFAE	0	0	0	0	0	0
OFL	0	0	0	0	0	0
SPr	0	0	0	0	0	0
COMCO	13	8	0	3	0	2
ZIVI	2	1	0	1	0	0
BFC	2	1	0	1	0	0
FNS	0	0	0	0	0	0
IFFP	0	0	0	0	0	0
CEPF	12	8	3	0	0	1
Total	**84**	**37**	**24**	**20**	**0**	**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	0	0	0	0	0	0
OFT	8	5	1	2	0	0
OFAC	14	2	7	4	1	0
OFEN	12	8	2	1	0	1
OFROU	6	3	0	1	0	2
OFCOM	11	8	2	4	0	3
OFEV	31	25	2	4	0	0
ARE	1	0	0	1	0	0
ComCom	1	1	0	0	0	0
IFSN	17	2	5	4	2	4
PostCom	1	0	1	0	0	0
AIEP	4	4	0	0	0	0
Total	**106**	**58**	**20**	**17**	**4**	**7**

Traitement des demandes d'accès



3.5 Statistique des demandes d'accès présentées auprès du Ministère public de la Confédération en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014)

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	6	5	1	0	0	0
Total	**6**	**5**	**1**	**0**	**0**	**0**

3.6 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2014 au 31 décembre 2014)

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	1	0	1	0	0	0
Total	**1**	**0**	**1**	**0**	**0**	**0**

3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2014 au 31 décembre 2014)

Catégorie de requérants	2014
Médias	44
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	19
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	9
Avocats	7
Entreprises	8
Universités	1
Communauté	2
Total	**90**

3.8 Secrétariat du PFPDT

Préposé fédéral à la protection des données et à la transparence:

	Thür Hanspeter, avocat
Suppléant:	Walter Jean-Philippe, Dr. iur.

Secrétariat:

Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité 1:	11 personnes
Unité 2:	14 personnes
Unité 3:	6 personnes (dont 2 stagiaires)
Chancellerie:	2 personnes