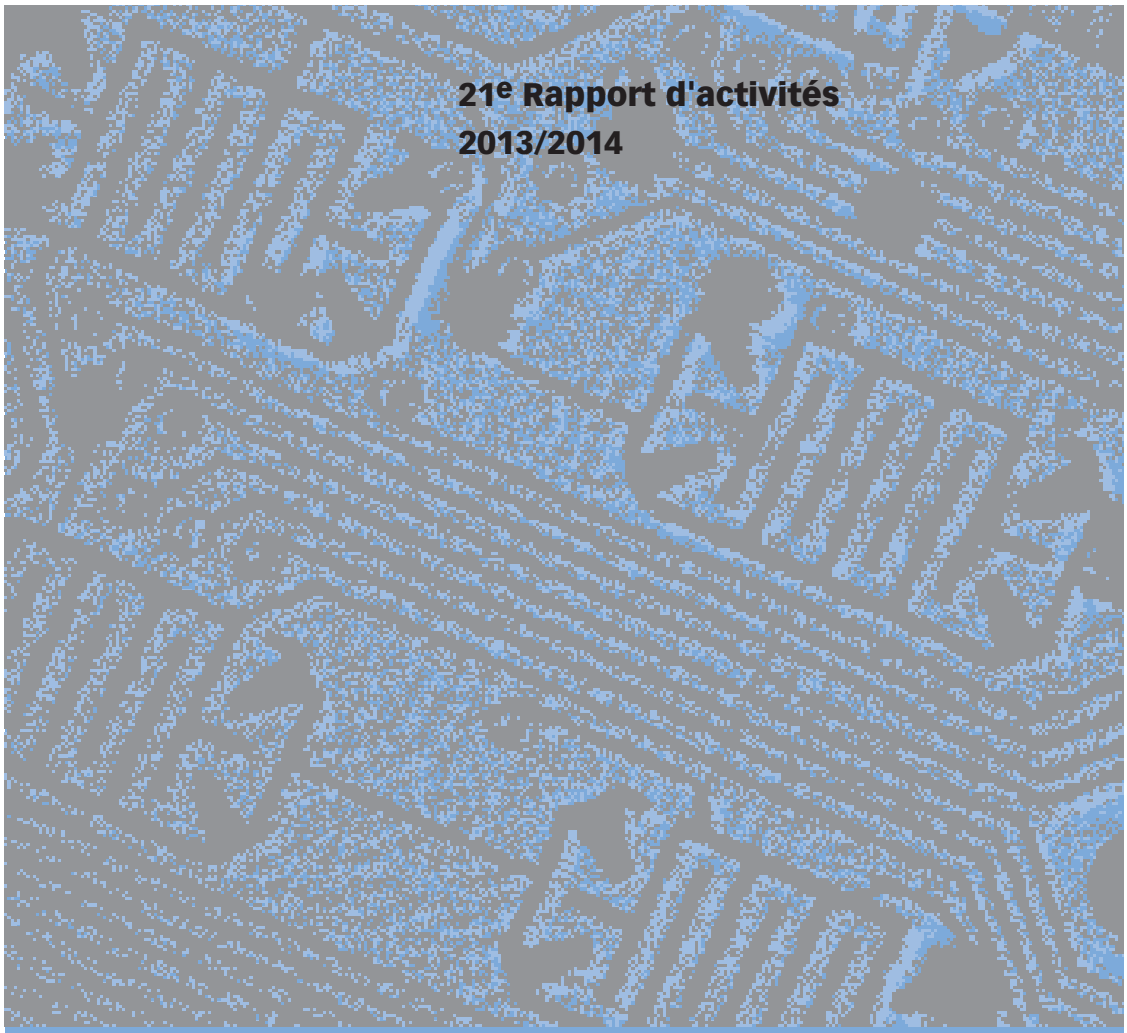


21e Rapport d'activités 2013/2014

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2013/2014 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 2013 au 31 mars 2014.

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. 410.021.d/f

Table des matières

Avant-propos – Bilan et perspectives

L'année dernière, je terminais mon avant-propos en évoquant l'importance grandissante des traitements massifs de données (Big Data). Compte tenu des progrès technologiques, des énormes capacités de stockage, de la possibilité de transmettre rapidement d'importants volumes de données partout dans le monde et de la précision d'analyse obtenue, les informations deviennent une véritable matière première (le nouveau capital?) dans une société future dirigée par les données. Ce développement implique une mise en danger massive de la vie privée.

S'il ne fallait choisir qu'un seul exemple, mondialement connu, nous citerions les révélations d'Edward Snowden, qui a livré quantité d'informations concernant les méthodes de surveillance de la NSA au travers des documents qu'il a rendus publics.

Il s'en est suivi un débat à l'échelle planétaire sur la surveillance massive, non seulement possible mais bel et bien pratiquée, visant les citoyens au niveau mondial. La phrase bien connue «Qui n'a rien à cacher n'a rien à craindre» apparaît ici dans toute sa naïveté. Ce qui est étonnant, c'est la grande indifférence avec laquelle citoyens et politiques tolèrent ce scandale.

Nous devons cependant accorder une attention majeure aux outils de surveillance étatique et réfléchir aux contre-stratégies possibles. En effet, une chose est évidente: «l'homme transparent» n'est plus une chimère, c'est une réalité, et ce depuis longtemps. La numérisation de notre environnement impose une conséquence inéluctable: toute donnée est tôt ou tard accessible, que nous le voulions ou non.

Sur la question de la surveillance tous azimuts, il serait facile, comme le font beaucoup de commentateurs, de se concentrer seulement sur les services secrets. Car ce sont à présent aussi les entreprises du secteur privé qui exploitent de grands volumes de données. Car les données, c'est du business, de l'argent, du pouvoir.

Les montagnes de données recueillies sur une base privée continuent de croître et constituent le matériau qui permet aux acteurs économiques d'enquêter sur chaque individu, jusque dans les moindres détails, sur ses préférences, ses caractéristiques, ses forces et ses faiblesses. Si le secteur privé effectue lui-même ce genre d'analyses, il ne faut alors pas s'étonner que les autorités étatiques – et la NSA en est une parmi d'autres – puisent dans les informations ainsi mises à disposition.

Ces masses de données sont une source réelle de préoccupation car les capacités immenses des ordinateurs et les procédures d'analyse automatisées permettent aujourd'hui d'obtenir des indications précises et de tirer des conclusions sur le comportement actuel et futur des individus. Les modèles ainsi dégagés conduisent parfois à des résultats impressionnants.

Les corrélations établies ne doivent pas obligatoirement avoir un lien logique. Si le volume de données est suffisamment grand, l'algorithme pourra par exemple mener à un modèle prédisant avec une probabilité élevée que celui qui porte des chaussures jaunes a le crâne dégarni! On pourrait certes objecter ici qu'à première vue, le fait qu'on puisse établir la probabilité selon laquelle un individu au crâne dégarni porte des chaussures jaunes est relativement anodin au premier abord.

Je rétorquerai que par ce biais, il est possible de découvrir des actes ou des traits de caractère compromettants sur les personnes. Et que cela peut être dangereux parce que l'algorithme ne constitue jamais une donnée sûre et n'exprime en tout cas pas une causalité fiable, scientifiquement contrôlable. Il s'agit toujours d'informations qui peuvent s'avérer justes, avec plus ou moins de vraisemblance. Lorsqu'un algorithme livre des informations sur un comportement potentiellement criminel, les conséquences peuvent se révéler dévastatrices pour la personne. La situation de Monsieur X devient pour le moins inconfortable lorsque d'après les données disponibles, les services secrets dégagent un algorithme qui l'identifie comme terroriste. À cela s'ajoute que le résultat de cet algorithme peut concerner de nombreuses autres personnes si l'on passe au crible de l'algorithme une grande quantité d'individus. C'est ainsi qu'opèrent les services secrets comme la NSA, que l'imprécision de ces analyses ne dérange d'ailleurs pas outre mesure.

Dans le même contexte, de plus en plus d'appareils ménagers et autres équipements techniques fonctionnent en réseau, souvent à l'insu de leur propriétaire, et communiquent entre eux. On parle de l'«Internet des objets»: ces objets envoient très discrètement des données à leurs fabricants qui, à leur tour, transmettent ces informations à des tiers. C'est ainsi que les téléviseurs informent les chaînes de télévision que tel téléspectateur change de chaîne. Il existerait même des «télévisions intelligentes» qui inspectent les disques durs lorsqu'ils sont mis en service et envoient un index des données recueillies aux fabricants. L'Internet des objets, le gros fournisseur en big data de demain!

Le débat qui entoure la réutilisation de données issues du secteur public (open data) relève du même contexte. Les pouvoirs publics pourraient devenir des fournisseurs de big data. S'il est incontesté que cela générerait des plus-values considérables pour l'économie et la société, l'utilisation de ces données présente cependant le risque qu'elles puissent être associées à une personne précise en les combinant avec des informations supplémentaires.

Quelles sont les implications de cet état de fait dans l'optique des travaux – déjà entamés – de révision de la loi sur la protection des données?

Les spécialistes s'accordent à dire que le Big Data constitue un défi de taille pour la protection des données car il comporte d'énormes risques. Les mécanismes

fondamentaux, techniques et légaux, de la protection des données sont vidés de leur substance. Comme le relèvent V. Mayer-Schönberger et K. Cukier, «Big Data»: «les big data peuvent faire de nous les prisonniers à vie de nos actes passés, lesquels sont utilisés contre nous lorsque des systèmes pensent pouvoir prédire notre comportement futur». Nous estimons qu'il faut examiner attentivement comment les principes fondamentaux de finalité et de transparence et les exigences relatives au consentement peuvent être respectés lorsque de grands volumes de données sont utilisés. Pouvons-nous par ailleurs autoriser l'exploitation d'importants stocks de données et leur interconnexion illimitée lorsqu'il s'agira de prendre, sur la base de probabilités, des décisions qui auront des répercussions négatives pour les individus?

Il ne fait aucun doute qu'à ce jour il n'existe aucun concept tant soit peu fiable sur la manière de répondre à ce défi. On pourrait par exemple examiner dans quelle mesure le droit fondamental numérique prôné par la juriste et auteure Juli Zeh est une voie envisageable. Pour elle, l'individu doit être seul maître de ses données personnelles et l'accès par des privés à son identité numérique ne doit être possible qu'avec son consentement. De plus, les interventions de l'État devraient être strictement limitées aux impératifs de la poursuite pénale.

De leur côté, Mayer-Schönberger et Cukier développent une autre approche: Ils proposent un contrôle formel, du point de vue de la protection de données, des applications du Big Data, mais requièrent en contrepartie que les exigences en matière de finalité et de consentement soient assouplies. Pour parer au danger que les prédictions des big data, ainsi que les algorithmes et les gros stocks de données sur lesquels elles reposent, deviennent une «boîte noire» sans responsabilités clairement établies, ils proposent de mettre en place une nouvelle autorité de contrôle. Telle une instance indépendante au même titre qu'un réviseur, un «algorithmicien» contrôlerait le choix des données, la qualité des instruments d'analyse et de prédiction, les algorithmes, les modèles mathématiques, ainsi que l'interprétation des résultats, et interviendrait si nécessaire.

La révision de la loi sur la protection des données s'impose d'urgence, car l'utilisation des big data est aujourd'hui un fait établi et remet en question des dispositions fondamentales de la loi actuelle. Il faut sans tarder mandater un groupe d'experts interdisciplinaire pour analyser la situation de manière approfondie et élaborer des solutions. Le Parlement a fait un premier pas dans cette direction en acceptant la motion Rechtsteiner. Une chose est sûre: si les politiques ne réagissent pas rapidement, le droit constitutionnel à la protection de la vie privée est menacé dans sa substance même!

Un dernier mot à propos de la loi sur la transparence: cette loi ayant été la cible de critiques de la part de différents acteurs de l'administration fédérale, l'Office

fédéral de la justice en a mandaté l'évaluation. À diverses reprises, il a été avancé que bon nombre de ses dispositions entravent l'activité de l'administration. Des unités administratives entières demandent même à être exclues de son champ d'application. Nous suivons cette évolution avec inquiétude. Cette loi a été adoptée par le Parlement dans le but de rendre l'activité de l'administration plus transparente et, par là, de renforcer la confiance des citoyens dans les institutions de l'État. Nous percevons actuellement de grandes réticences dans le domaine des adjudications de marchés publics et des subventions lorsque la divulgation des documents concernés est demandée. À cet égard, le scandale qui a récemment secoué le SECO a montré de manière brutale la nécessité d'une plus grande transparence.

Liste des abréviations

ACC	Autorité de contrôle commune de Schengen
AFAPDP	Association francophone des autorités de protection des données
AFC	Administration fédérale des contributions
AFD	Administration fédérale des douanes
AOS	Assurance obligatoire des soins
ASR	Autorité fédérale de surveillance en matière de révision
ATF	Arrêt du Tribunal fédéral
CCT	Convention collective de travail
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CDI CH-USA	Convention entre la Confédération suisse et les États-Unis d'Amérique en vue d'éviter les doubles impositions en matière d'impôts sur le revenu
CEDH	Cour européenne des droits de l'homme
CER	Commission de l'économie et des redevances du Conseil des États
ChF	Chancellerie fédérale
CNIL	Commission nationale de l'informatique et des libertés
CNPT	Commission nationale de prévention de la torture
COMCO	Commission de la concurrence
DDC	Direction du développement et de la coopération
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFE	Département fédéral de l'économie
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DRG	Diagnoses Related Groups

ESTI	Inspection fédéral des installations à courant fort
Eurodac	Système d'information pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin
FINMA	Autorité fédérale de surveillance des marchés financiers
FNS	Fonds national suisse de la recherche scientifique
GAFI	Groupe d'action financière
IFSN	Inspection fédérale de la sécurité nucléaire
IRS	Internal Revenue Service
ISO/CEI	ISO / Commission électrotechnique internationale
LAMal	Loi fédérale sur l'assurance-maladie
LBA	Loi sur le blanchiment d'argent
LCA	Loi fédérale sur le contrat d'assurance
LDEIP	Loi fédérale sur le dossier électronique du patient
LERI	Loi fédérale sur l'encouragement de la recherche et de l'innovation
LPD	Loi fédérale sur la protection des données
LPers	Loi sur le personnel de la Confédération
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
LRens	Loi sur le renseignement
LRH	Loi relative à la recherche sur l'être humain
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
LTV	Loi sur le transport de voyageurs
MPC	Ministère public de la Confédération
NAVS13	Numéro AVS à 13 chiffres
N-SIS	Partie nationale du Système d'information Schengen
OAMal	Ordonnance sur l'assurance-maladie
ODM	Office fédéral des migrations
OEC	Ordonnance sur l'état civil
OFAC	Office fédéral de l'aviation civile

OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFCL	Office fédéral des constructions et de la logistique
OFEC	Office fédéral de l'état civil
OFEN	Office fédéral de l'énergie
OFEV	Office fédéral de l'environnement
OFJ	Office fédéral de la justice
OFL	Office fédéral du logement
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
OFT	Office fédéral des transports
OLT3	Ordonnance 3 relative à la loi sur le travail (Hygiène)
OPrI	Ordonnance concernant la protection des informations de la Confédération
OTrans	Ordonnance sur le principe de la transparence dans l'administration
PA	Loi fédérale sur la procédure administrative
PFPDT	Préposé fédéral à la protection des données et à la transparence
PIN	Personal Identification Number
PNR	Programme national de recherche
POS	Point of Sale
RFID	Radio Frequency Identification
RIP	Réduction individuelle des primes
SAS	Service d'accréditation suisse
SCHEVAL	Groupe de travail du Conseil «SCHEVAL» (pour SCHengen EVALuation Working Party)
SECO	Secrétariat d'État à l'économie
SFI	Secrétariat d'État aux questions financières internationales
SIS	Système d'information Schengen
SIS II	Système d'information de Schengen II
SMR	services médicaux régionaux

SRC	Service de renseignement de la Confédération
SRD	Service de réception des données
Swissmedic	Institut suisse des produits thérapeutiques
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
UTP	Union des transports publics
VIS	Système d'information sur les visas

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Accompagnement d'audits de réaccréditation des certificateurs de protection des données

Nous avons été associés à des audits de réaccréditation conduits par le Service d'accréditation suisse lors de certification de services de réception de données d'un assureur-maladie. Cela a été pour nous l'occasion de constater la validité de la certification organisationnelle dans ce contexte particulier et de préciser aux certificateurs nos exigences spécifiques en matière de périmètre et d'étendue, de qualification du personnel, de composition d'équipe et de contenu des rapports d'audit.

Dans le cadre de la procédure de réaccréditation des certificateurs d'organisation ou de procédure en matière de protection des données, le service d'accréditation suisse (SAS) a assisté à la certification des services de réception de données (SRD) de deux assureurs-maladie, réalisées par les deux certificateurs actuellement accrédités pour le marché suisse. L'ordonnance sur l'assurance-maladie dispose en effet que chaque assureur doit, à partir du 1er janvier 2014 selon les dispositions transitoires, disposer d'un SRD certifié. Seul ce dernier obtient l'accès aux informations médicales transmises par le fournisseur de prestations avec la facture et d'autres données administratives. Il détermine ainsi pour quelles factures un examen plus approfondi est nécessaire et transmet à l'assureur les informations pertinentes. Nous avons été associés à ces audits de réaccréditation conformément à l'ordonnance sur les certifications en matière de protection des données, ce qui nous a permis de constater que l'actuelle certification organisationnelle permettait d'apporter des garanties essentielles quant au respect des principes fondamentaux de protection des données pour l'ensemble du traitement des SRD des assureurs. Cela étant, nous avons profité de cette occasion pour bien préciser aux certificateurs, avec l'appui du SAS, nos attentes spécifiques quant à la certification désormais obligatoire de ces SRD des assureurs-maladie, à savoir:

- Le périmètre doit couvrir, chez l'assureur comme chez d'éventuels prestataires de service, tous les processus nécessaires à l'accomplissement des tâches du SRD, y compris toutes ses interfaces avec les systèmes environnants.
- L'étendue de l'audit comprend l'ensemble des contrôles que nous avons définis pour l'ensemble du système de gestion de protection des données. La norme ISO/CEI 27006 «Exigences pour les organismes procédant à

l'audit et à la certification des systèmes de management de la sécurité de l'information», fournit par ailleurs de précieuses indications quant à l'estimation du temps requis, à la qualification du personnel impliqué et au contenu des documents et rapports d'audit.

- L'équipe d'audit doit réunir les compétences d'un auditeur principal expérimenté, d'un expert en protection des données spécialiste des questions d'assurance-maladie et d'un expert en sécurité de l'information.

Pour conclure, nous sommes d'avis que ces démarches vont certainement contribuer à améliorer le respect des exigences de protection des données dans les SRD certifiés (voir la liste publiée sur notre site www.leprepose.ch, sous la rubrique Protection des données – certifications).

1.1.2 Révision partielle de l'ordonnance sur les relevés statistiques

Le Conseil fédéral a approuvé la révision partielle de l'ordonnance sur les relevés statistiques. Lors des procédures de consultation, nous avons salué les efforts entrepris en vue de rendre le texte le plus clair et transparent possible. Nous avons toutefois rappelé la nécessité d'établir un règlement de traitement et de mettre en route des travaux législatifs relatifs à la loi fédérale sur la statistique afin de permettre une règlementation uniforme et transparente du numéro AVS dans les relevés statistiques.

Le 18 décembre 2013, le Conseil fédéral a approuvé la révision partielle de l'ordonnance sur les relevés statistiques. Les modifications sont entrées en vigueur le 15 janvier 2014. L'ordonnance révisée règle dans quelles conditions et sous quelle forme les appariements de données sont autorisés. Les différentes statistiques sont présentées dans l'annexe de l'ordonnance. Cette annexe est révisée chaque année, créant ainsi la base légale nécessaire à l'adaptation et à la mise à jour régulières des statistiques. Dans le cadre de la révision de l'ordonnance, les appariements de données prévus ont été indiqués pour chaque statistique concernée, par souci de transparence.

Nous avons été invités au préalable à prendre position sur ladite ordonnance et son annexe. Nous avons pu constater que la plupart de nos remarques formulées à l'occasion d'une première consultation (cf. notre 20e rapport d'activité 2012/2013, ch. 1.1.1) avaient été prises en compte, en particulier nos remarques concernant les phases de pseudonymisation/anonymisation, la destruction du matériel d'enquête; de même, nous avons salué les efforts entrepris en vue de rendre l'appariement de données le plus clair et transparent possible.

Nous avons toutefois rappelé la nécessité d'établir un règlement de traitement décrivant notamment le processus du Key Management et de mettre en route la révision de la loi fédérale sur la statistique afin de permettre une règlementation uniforme et transparente du numéro AVS dans les relevés statistiques. Nous avons aussi rappelé la nécessité d'examiner, dans le cadre de ces travaux législatifs, des méthodes de chiffrement, respectivement de pseudonymisation, du numéro AVS utilisé à des fins statistiques.

Au terme de la procédure de consultation, nous avons pu mesurer l'intérêt de certains offices fédéraux à pouvoir apparier eux-mêmes leurs données avec celles de l'Office fédéral de la statistique (OFS). L'état actuel de la loi sur la statistique fédérale ne permet aucune interprétation extensive et seuls l'Office OFS et les services cantonaux et communaux de statistique sont autorisés à apparier les données de l'OFS pour exécuter leurs tâches en matière statistique. Si d'autres organes fédéraux envisagent d'apparier leurs données à celles de l'OFS, une modification de la base légale serait alors indispensable.

1.1.3 Le projet MARS de l'Office fédéral de la statistique

Nous avons pris connaissance du lancement du projet MARS de l'Office fédéral de la statistique (OFS). L'objectif du projet est d'obtenir un système d'information statistique intégral sur la santé fournissant certaines données sur les établissements, les fournisseurs de prestations et les patients. Nous suivons le projet avec attention.

Le projet MARS (Modules ambulatoires des Relevés sur la Santé) de l'OFS résulte de la modification de l'ordonnance sur l'assurance maladie (OAMal), successivement à la révision partielle de la loi fédérale sur l'assurance maladie (LAMal), chargeant l'OFS de collecter auprès des fournisseurs de prestations des données pour les statistiques des soins ambulatoires.

Les données actuellement disponibles dans le secteur ambulatoire sont incomplètes. L'objectif du projet est donc d'obtenir un système d'information statistique intégral sur la santé fournissant certaines données sur les établissements, les fournisseurs de prestations et les patients afin de répondre aux besoins statistiques selon la loi fédérale sur la statistique, ainsi qu'aux tâches exécutives de la Confédération ou des cantons au sens de la LAMal. Ainsi, les données actuellement disponibles dans le secteur des soins stationnaires seront complétées par des données sur les prestations dans le secteur ambulatoire.

Au vu de la nature sensible des données personnelles collectées, nous restons particulièrement attentifs au développement du projet. 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. Un règlement de traitement doit en plus être élaboré afin de préciser les processus de traitement.

Différents sous-projets sont prévus et doivent être réalisés par étapes. Des essais pilotes sont prévus pour 2014. Nous continuons de suivre le projet avec attention car nous avons pu constater qu'un certain nombre de points, tant juridiques que techniques, restent encore ouverts à ce stade.

1.1.4 Thinkdata: travaux du groupe opérationnel

Dans le cadre de nos activités de sensibilisation, nous restons actifs dans le projet Thinkdata. Le projet suit son cours et est entré dans sa phase opérationnelle qui est supervisée par nos soins. Parallèlement, le groupe de travail qui se penche sur la suite stratégique du projet a mis ses activités entre parenthèses.

Pour faire évoluer le service de sensibilisation à la protection des données et à la transparence Thinkdata (www.thinkdata.ch), nous avons pris la tête d'un groupe opérationnel composé de plusieurs représentants des autorités de protection des données cantonales ainsi que d'autres membres d'horizons divers, tels que le secteur privé et le monde politique. Le groupe opérationnel s'est réuni plusieurs fois durant l'année pour discuter de l'avenir de Thinkdata mais également pour adapter certaines fonctionnalités du site afin de répondre aux besoins tant des utilisateurs que des fournisseurs du service.

Plusieurs nouveaux scénarios ont été développés (en français essentiellement) et mis en ligne sur le site. Le nombre de visiteurs reste stable et des nouvelles propositions de scénarios arrivent régulièrement par le biais du formulaire de contact disponible sur le site.

En collaboration avec les préposés cantonaux, nous souhaitons faire de Thinkdata un service des autorités de protection des données et redéfinir la composition du groupe opérationnel.

1.2 Protection des données – Questions d'ordre général

1.2.1 Stockage centralisé des photos de clients dans les stations de ski – Clôture de la procédure

La station de ski que nous avons inspectée a procédé à toutes les modifications requises pour rendre l'exploitation de son système de contrôle d'accès conforme aux exigences de la protection des données. Nous avons ainsi pu clore la procédure d'examen des faits.

La pratique de contrôle d'accès exercée par de nombreuses stations de ski à l'aide de cartes d'abonnement munies de photos ayant suscité de vives critiques, nous avons vérifié la conformité de ces systèmes avec les exigences de la protection des données (cf. notre 18e rapport d'activités 2010/2011, ch. 1.2.5). Pour ce faire, nous avons tout d'abord procédé à un examen des faits auprès d'une station de ski concernée, au cours duquel nous avons constaté plusieurs lacunes dans l'application des principes de traitement de la protection des données. Certaines de ces lacunes étaient inhérentes au système utilisé par la plupart des stations de ski suisses (cf. notre 19e rapport d'activités 2011/2012, ch. 1.2.9).

Le fabricant du système a donc accepté de réaliser dans les meilleurs délais les améliorations techniques que nous avons demandées (cf. notre 20e rapport d'activités 2012/2013, ch. 1.2.2). D'autres défauts étaient dus à la manière dont la station de ski contrôlée a utilisé le système. Ainsi, les personnes concernées n'ont pas été suffisamment informées quant aux traitements effectués avec leurs données. Il n'existait par exemple pas de délai de conservation des données stockées, et les droits d'accès n'étaient pas clairement réglés. La station de ski a entre-temps apporté les modifications nécessaires pour rendre l'exploitation du système conforme aux exigences de la protection des données. Elle a ainsi rempli toutes nos exigences, de sorte que la procédure d'examen des faits a pu être close.

1.2.2 Vidéosurveillance à des fins de recherche

Lorsque des personnes participant à un projet de recherche sont filmées, la protection de leur personnalité est assez simple à respecter. Par contre, lorsque des tiers qui ne sont pas directement impliqués sont filmés dans le cadre d'un tel projet, il y a lieu de prendre certaines précautions pour garantir la protection des données.

L'utilisation d'une caméra vidéo dans le cadre d'un projet de recherche permet d'enregistrer et d'analyser le comportement de personnes déterminées. Les données obtenues de cette manière sont souvent bien plus précises que celles

que l'on recueille par exemple au moyen d'un questionnaire. Si les caméras ne filment que les personnes participant au projet de recherche, les principes de traitement de la protection des données peuvent relativement facilement être appliqués, minimisant ainsi le risque d'atteinte à la personnalité. Ceci est dû au fait que les personnes concernées participent en règle générale volontairement au projet de recherche, qu'elles savent qu'elles sont filmées et sont informées sur les traitements prévus avec leurs données, ou peuvent du moins être informées par la suite en détail sur le projet de recherche.

La situation est plus compliquée dans les cas où les caméras sont utilisées dans des espaces accessibles au public et peuvent ainsi filmer des tiers qui ne sont pas directement impliquées dans le projet de recherche. Il serait faux d'admettre que les images de passants fortuits ne constituent pas des données personnelles, simplement parce que l'on ne connaît pas le nom de ces personnes. Ces images pouvant être attribuées à des personnes déterminées, elles doivent clairement être considérées comme des données personnelles; les principes de traitement de la protection des données doivent donc également être respectés dans ces cas.

Un traitement de données personnelles à des fins de recherche peut certes être justifié même sans le consentement des personnes concernées, dès lors que les finalités de l'étude ne se rapportent pas à des personnes et que les résultats de recherche publiés ne permettent pas d'identifier les personnes concernées. Ce privilège réservé aux projets de recherche ne dispense cependant pas d'informer sur le traitement de données, ce qui peut s'avérer difficile à mettre en œuvre lors d'un tournage dans un espace public. Ainsi, les passants qui pénètrent accidentellement dans le champ de vision de la caméra ne réalisent que leurs données sont traitées qu'au moment où elles aperçoivent la caméra, ce qui est trop tard puisque l'enregistrement est déjà en cours, voire déjà terminé.

Afin de préserver les droits de la personnalité de ces personnes, il convient de respecter les points suivants:

L'application du privilège réservé à la recherche implique que les enregistrements vidéo contenant des personnes identifiables ne soient pas publiés ou qu'ils soient préalablement altérés de sorte que personne ne puisse plus être identifié. Il est important de noter dans ce contexte qu'il ne suffit souvent pas de masquer simplement les yeux car il est possible d'identifier une personne en observant sa démarche, les vêtements qu'elle porte, etc.

Dans la mesure du possible, on rendra le public attentif aux prises de vue en apposant des panneaux bien visibles qui indiquent également à qui on peut s'adresser pour obtenir plus d'informations ou pour faire valoir ses droits à obtenir un accès ou à faire effacer ses données. Dans les cas où cela n'est pas possible, on

créera un support d'information standardisé – tel qu'un dépliant ou une brochure – qui pourra être remis sur place. Ce dépliant devrait non seulement couvrir tous les points importants du traitement de données, mais aussi contenir les coordonnées de contact susmentionnées. Les personnes concernées doivent pouvoir faire valoir leurs droits d'accès et d'effacement simplement et sans frais.

Le privilège réservé aux projets de recherche ne permet en aucun cas de justifier des enregistrements vidéo des parties intimes du corps. Cela signifie que, même pour les projets de recherche, les enregistrements dans des toilettes, vestiaires, etc. ne sont pas autorisés sans le consentement des personnes concernées.

1.2.3 Remise d'enregistrements vidéo aux autorités de poursuite pénale

L'exploitant d'un système de vidéosurveillance peut sans autre transmettre des images demandées sur la base d'une décision. Dans les cas où une telle demande n'est pas fondée sur une décision, il ne pourra fournir les données qu'après avoir soigneusement examiné la situation. Il est responsable de la licéité de la remise des images.

L'exploitant d'un système de vidéosurveillance qui reçoit une demande émanant d'une autorité de poursuite pénale dans le cadre d'une procédure peut transmettre les enregistrements vidéo à cette dernière en se fondant sur la décision de l'autorité. La remise des images est dans ce cas justifiée.

En l'absence de procédure pénale, il importe de déterminer si la démarche présente un intérêt public prépondérant qui justifierait la transmission d'enregistrements. Une pondération des intérêts en présence permettra de répondre à la question. Toutefois, le choix de transmettre des enregistrements vidéo peut être délicat; il convient de prendre en compte les considérations suivantes:

- Vérifier tout d'abord qui exige la remise. S'il n'existe pas de décision, ne remettre les images qu'à des autorités de poursuite pénale. Pour d'autres autorités ou pour des demandeurs privés, exiger toujours une décision.
- Ensuite, l'exploitant doit vérifier à quelles fins il est prévu d'utiliser les images. Cela signifie que la demande écrite doit toujours contenir un exposé des motifs. Une remise sans décision n'est justifiée que si elle permet de protéger des intérêts majeurs. Toute demande non motivée ou servant des objectifs peu importants devrait être refusée par l'exploitant. Étant donné qu'il peut être tenu responsable s'il remet des enregistrements vidéo sans la présence d'une décision ou d'un intérêt prépondérant, il doit en cas de doute demander une décision.

- Toutefois, si l'exploitant d'un système de surveillance vidéo conclut qu'une remise est justifiée, il doit visionner les enregistrements et en extraire les séquences qui sont pertinentes pour la demande. Seules ces séquences seront alors transmises.

De plus amples informations à ce sujet ont été publiées sur notre site web www.leprepose.ch, dans la rubrique Protection des données – Surveillance vidéo sous le lien «Explications sur la transmission d'enregistrements vidéo aux autorités de poursuite pénale».

1.2.4 Saisie d'interdictions d'entrée sur une liste noire

Les boîtes de nuit sont en principe autorisées à saisir sur une liste noire interne les données personnelles des personnes interdites d'entrée dans leur établissement. La communication de ces données à d'autres boîtes de nuit ne peut être justifiée qu'au cas par cas. La communication systématique à des tiers par le biais d'une banque de données centrale est par conséquent problématique.

Dans le cadre de nos activités de conseil, nous avons examiné la conformité, du point de vue de la loi sur la protection des données, d'une banque de données centralisée dans le domaine des boîtes de nuit. Nous avons constaté que des modifications étaient nécessaires et avons contacté les personnes responsables pour leur faire part de nos propositions d'amélioration.

Boîtes de nuit ou discothèques peuvent prononcer des interdictions d'entrée. Afin de faire respecter ces interdictions, les établissements saisissent les données personnelles des clients indésirables sur une liste noire et procèdent à des vérifications d'identité. Un tel traitement de données est en principe justifié par un intérêt privé prépondérant, dans la mesure où les principes généraux de la loi sur la protection des données (LPD) sont respectés. Le comportement fautif de visiteurs de la boîte de nuit figurant dans un tel fichier pouvant également avoir des suites pénales, on doit présumer qu'une telle liste noire contient des données sensibles. Le traitement de telles données doit en conséquence remplir des exigences plus sévères, notamment au niveau de la sécurité des données et du devoir d'information.

Si les divers établissements font partie d'une même association et qu'ils désirent saisir les informations personnelles dans une banque de données centrale à laquelle tous les établissements ont accès, ceci constitue une communication à des tiers au sens de la LPD. Cette communication n'ayant plus pour but de faire respecter une interdiction d'accès prononcée, elle nécessite un nouveau motif justificatif. Il y a donc lieu d'examiner au cas par cas si un intérêt prépondérant privé ou public

justifie la divulgation à des tiers. C'est généralement (seulement) le cas lorsque le comportement fautif de la personne concernée revêt une certaine gravité et que l'on dispose d'un soupçon concret que la personne réitérera ce comportement dans d'autres établissements. La communication n'est cependant pas justifiée par exemple en cas de problème personnel avec un employé particulier.

La communication systématique et automatisée, entre les boîtes de nuit, des données recueillies dans le cadre d'interdictions d'entrée prononcées par d'autres établissements peut donc s'avérer problématique. La saisie de données dans un fichier central accessible à tous les établissements correspond à une communication de données personnelles à des tiers. Il n'est pas possible de vérifier à chaque accès s'il existe un motif justificatif.

La responsabilité concernant la licéité du traitement de données ainsi que la pesée des intérêts incombe à chacun des établissements. Il est cependant possible de déléguer le traitement des données à un tiers dans le cadre d'un contrat de sous-traitance. Dans un tel cas, le mandataire ne peut effectuer que les traitements de données que le mandant serait lui-même autorisé à effectuer. S'il travaille pour le compte de plusieurs établissements, il devra en particulier veiller à ce que la liste noire reste interne et que les données ne soient pas accessibles aux autres, et prendre des mesures techniques et organisationnelles correspondantes. Ce n'est que s'il dispose d'un motif justificatif dans le cas d'espèce que le mandataire pourra transmettre les données concernées aux autres établissements, par exemple par le biais d'une banque de données centrale.

Nous avons demandé des adaptations afin d'assurer la conformité avec les exigences de la protection des données: une séparation claire doit notamment être faite entre les listes noires internes, auxquelles seul l'établissement respectif peut avoir accès, et la banque de données commune. Un règlement de traitement doit être élaboré pour la liste noire interne, un autre pour la liste noire commune. La saisie de données dans la liste commune doit être soumise à des critères stricts. Il doit s'agir d'incidents d'une certaine gravité. De plus, il convient de procéder à un examen du risque de récidive dans chaque cas d'espèce. Les traitements de données effectués par des tiers requièrent la conclusion d'un contrat de sous-traitance.

1.2.5 Introduction d'une carte électronique dans les transports publics

Lors d'une réunion avec l'Union des transports publics et les CFF, nous avons assisté à une démonstration de la carte électronique pour les transports publics (carte TP). L'introduction est prévue à partir de 2015 et s'effectuera par étapes. Différents points n'ont pas encore pu être réglés.

Comme nous avons pu lire dans un communiqué de presse publié par l'Union des transports publics (UTP) et les CFF, il est prévu d'introduire à la mi-2015 la carte électronique pour les transports publics, qui intégrera la technologie RFID. Le communiqué de presse mentionnait que les exigences de la protection des données suisse seraient remplies. Pour vérifier ceci, nous avons demandé que l'UTP et les CFF nous présentent ce projet à l'occasion d'une réunion. Il est prévu, dans une première étape, d'intégrer une puce RFID dans les abonnements. Cette puce contiendra un numéro d'identification, mais pas de nom ni de prénom. Ces données seront utilisées principalement à des fins de contrôle. L'UTP et les CFF nous ont assuré qu'ils nous tiendraient informés de l'évolution de ce projet. Nous suivrons les étapes à venir et prendrons régulièrement position sur les aspects relevant de la protection des données.

1.2.6 Voyageurs sans titre de transport valable

Suite au contrôle que nous avions effectué auprès des CFF concernant les voyageurs sans titre de transport valable, nous avons procédé à un contrôle a posteriori et vérifié la suppression des données. Nous avons également pris position sur le projet de base légale pour le système d'information.

Dans le cadre de notre contrôle concernant les voyageurs sans titre de transport valable, nous avions constaté que les CFF n'avaient supprimé aucune donnée, malgré le fait qu'il était prévu de ne conserver les données que pour une durée de deux ans (cf. notre rapport d'activités 2012/2013, ch. 1.2.3). Après que les CFF ont accepté nos recommandations et nous ont soumis un concept pour la suppression ainsi que le règlement de traitement, nous avons effectué une vérification sur place. Nous avons à cette occasion pu constater que toutes les données dont le délai de conservation était expiré avaient été supprimées dans le système d'information. Les données supprimées concernent 1,85 million de trajets, près de 0,72 million de voyageurs et environ 2,7 millions d'enregistrements issus des terminaux mobiles pour le personnel roulant. De même, les «formulaires 7000» numérisés qui avaient été conservés trop longtemps ont également été éliminés.

Lors de notre contrôle, nous avons en outre constaté que la loi sur le transport des voyageurs (LTV) réglementait la perception du supplément pour les voyageurs sans titre de transport valable, mais pas le système d'information lui-même. L'Office fédéral des transports (OFT) nous avait confirmé qu'il entamerait les démarches nécessaires à la création de la base légale manquante. L'OFT a ensuite inclus cette base légale dans un paquet de lois déjà existant («Conditions d'admission des entreprises de transport par route et dispositions pénales en droit des transports») comme nouvel article 20a LTV. Nous avons pris position sur ce projet et proposé

quelques modifications, qui ont en principe été prises en compte. L'ensemble du paquet de lois a été traité par le Conseil fédéral en septembre 2013 et sera débattu au Parlement.

1.2.7 Drones et protection des données

Nous avons eu une réunion avec l'Office fédéral de l'aviation civile concernant les drones équipés de caméras et avons été entendus à ce sujet par la Commission des transports et des télécommunications du Conseil national. Nous sommes d'avis que la situation des drones doit être examinée de manière plus approfondie du point de vue de la protection des données et qu'il faudrait prévoir des réglementations ou des autorisations spéciales.

On trouve sur le marché de plus en plus de drones à des prix abordables et faciles à manier. Les drones sont des avions télécommandés, généralement de petite taille, qui du point de vue juridique sont assimilés aux modèles réduits. Une autorisation n'est pas nécessaire tant que leur poids ne dépasse pas 30 kilos et que le pilote a en tout temps un contact visuel avec son drone. Les drones sont de plus en plus souvent équipés d'une caméra et utilisés aussi bien à des fins privées que commerciales.

Il est très simple de survoler et de filmer des jardins, bâtiments ou bureaux privés avec un drone. Les drones permettent en outre de faire des enregistrements vidéo dans des lieux qui ne sont pas accessibles à pied. Les prises de vues peuvent être effectuées à l'insu des personnes concernées. Dans certains cas, le drone n'est découvert qu'alors qu'il est déjà en train de filmer. De plus, il n'est pas toujours possible d'identifier la personne qui pilote le drone. Dans certains cas, les pilotes ne sont même pas conscients du fait que ce qu'ils font est illicite (et éventuellement même punissable), dans d'autres ils en assument le risque. Les images prises peuvent très facilement être publiées, ce qui amplifie la problématique en matière de protection des données.

Au vu de cette problématique, nous avons formulé les exigences à respecter en matière de protection des données et avons publié des explications sur ce thème sur notre site www.leprepose.ch, sous la rubrique Protection des données – technologies – vidéosurveillance.

De plus, nous avons eu un entretien à ce sujet avec l'Office fédéral de l'aviation civile (OFAC) et l'Office fédéral de la justice (OFJ). Nous avons également été entendus par la Commission des transports et des télécommunications du Conseil national. Lors de cette séance, tous les participants ont partagé l'avis qu'une difficulté majeure rencontrée en cas d'utilisation de drones était de faire respecter les droits des personnes concernées. La Commission a décidé de se limiter, pour le moment, à observer la situation.

Nous sommes d'avis que l'aspect de la protection des données dans l'utilisation de drones équipés de caméras devrait être examiné de plus près. Il faudrait, dans ce cadre, examiner s'il y a lieu d'édicter des réglementations spéciales ou de prévoir un régime d'autorisation préalable et examiner comment le grand public pourrait être sensibilisé à ce problème.

1.2.8 Révision partielle de la loi fédérale sur la radio et la télévision

Conformément au projet de révision partielle de la loi fédérale sur la radio et la télévision, une nouvelle base légale doit être créée pour le relevé des données sur les ménages provenant des registres des habitants, en particulier le numéro d'assuré (NAVS13). Comme nous l'avons souligné au cours de la consultation des offices, cette utilisation des numéros d'assurés renferme un risque de couplage des banques de données.

Au cours de l'année sous revue, nous nous sommes exprimés sur le projet de révision partielle de la loi fédérale sur la radio et la télévision (LRTV). Nous avons émis des remarques sur le traitement de données par l'organe de perception, en particulier sur les données sensibles, ainsi que sur le cryptage de ces données. Nos remarques ont été prises en compte dans le texte de loi.

Néanmoins, une divergence avec l'office fédéral chargé de la révision n'a pas pu être éliminée. Celle-ci concerne l'utilisation du numéro d'assuré (NAVS13) provenant des registres des habitants. Dans notre appréciation du projet de loi, nous sommes parvenus à la conclusion que l'utilisation du numéro AVS n'est pas nécessaire à la perception de la redevance, qu'elle ne constitue pas le moyen le moins intrusif et que la proportionnalité au sens strict n'est pas garantie. Il convient donc d'y renoncer. En particulier, la mise en œuvre au niveau national d'un identificateur de personnes dans l'administration (Confédération, cantons, communes) crée les conditions techniques permettant la mise en commun d'informations personnelles extraites de banques de données touchant les domaines de la vie les plus divers. Or les interconnexions indésirables ou interdites de données peuvent induire de considérables atteintes à la personnalité. Donc, toute utilisation systématique du numéro d'assuré en dehors de l'assurance sociale doit répondre aux impératifs de nécessité et de proportionnalité.

Nous avons proposé d'utiliser à la place un numéro sectoriel calculé sur la base du NAVS13 (numéro AVS haché). Cette conversion au moyen d'une fonction unidirectionnelle permettrait de ne plus déterminer le numéro d'origine, ce qui réduirait considérablement le problème de l'interconnexion de différentes banques de données.

1.2.9 Révision totale de la loi sur les systèmes d'information de la Confédération dans le domaine du sport

Dans le cadre de la procédure de consultation des offices, nous nous sommes prononcés sur les projets de révision totale de la loi fédérale sur les systèmes d'information de la Confédération dans le domaine du sport. En particulier, nous nous sommes exprimés sur la nécessité du consentement des sportifs et sur le rajout de certaines catégories de données personnelles dans le système d'information de l'Agence nationale de lutte contre le dopage.

La loi fédérale sur les systèmes d'information de la Confédération dans le domaine du sport est entrée en vigueur en octobre 2012. Depuis, y ont été rajoutés le système de traitement des résultats du diagnostic de performance, le système d'évaluation systématique des cours et des formations ainsi que le système de l'Agence nationale de lutte contre le dopage. Ils nécessitent tous une base légale formelle. Nous nous sommes prononcés sur le projet de loi et sur le message.

D'une part, nous avons obtenu que la disposition concernant la communication de données et de résultats du diagnostic de performance soit complétée dans les commentaires explicatifs, à savoir que toute communication de données nécessite le consentement du sportif concerné qui a été au préalable informé.

D'autre part, sur la base de notre requête, toutes les catégories de données personnelles gérées dans le système d'information de l'Agence nationale de lutte contre le dopage ont été mentionnées. En principe, seul le traitement de données sensibles et de profils de la personnalité nécessitent une base légale formelle. Pour toutes les autres catégories, une base légale au niveau de l'ordonnance serait suffisante. La liste de toutes les catégories de données personnelles contribue à une meilleure compréhension du système d'information.

1.2.10 Publication de données d'état civil sur Internet

Nous avons conseillé l'Office fédéral de l'état civil sur les aspects de protection des données liés à la publication de données d'état civil sur Internet. Nous avons dans ce contexte attiré l'attention sur la perte de contrôle, sur la durée excessivement longue du traitement de ces données par des tiers et sur les éventuelles modifications de la finalité du traitement des données.

Dans le cadre des modifications prévues à l'article 57 de l'ordonnance sur l'état civil (OEC), l'Office fédéral de l'état civil (OFEC) nous a demandé conseil. Cette disposition réglemente la publication de données d'état civil par les cantons. Ceux-ci peuvent régler eux-mêmes la publication de naissances, décès, mariages ou enregistrements

de partenariat. Il s'ensuit que les cantons ont aménagé les dispositions légales pour la publication de ces données de manière diverse. Nous avons surtout rendu l'OFEC attentif aux risques liés à une publication sur Internet, comme par exemple la perte du contrôle des données. En outre, les données sont traitées plus longtemps qu'il ne l'était prévu à l'origine, à des fins les plus diverses et elles sont mises en relation avec d'autres données pour créer des profils de la personnalité, pour ne citer que quelques-uns des aspects que nous avons présentés. C'est pour les mêmes raisons que nous considérons comme problématique la publication illimitée dans le temps sur Internet de données du registre du commerce, cf. chiffre 1.8.4 du présent rapport d'activités.

1.2.11 Publication de mesures de protection des adultes

Nous avons, suite à une demande de la Commission des affaires juridiques du Conseil national, expliqué comment procéder pour qu'une publication de mesures de protection des adultes soit conforme aux exigences de la protection des données et que la sécurité du droit puisse être garantie dans les relations d'affaires.

La Commission des affaires juridiques du Conseil national nous a demandé de prendre position sur l'initiative parlementaire de Rudolf Joder visant à modifier la publication des mesures de protection des adultes. Le nouveau droit sur la protection des adultes, qui est en vigueur depuis 2013, ne prévoit plus, contrairement au droit précédent, que ces mesures soient publiées. Certes, l'article 451 du Code civil permet à toute personne dont l'intérêt est rendu vraisemblable de demander à l'autorité de protection des adultes qu'elle lui indique si une personne déterminée fait l'objet d'une mesure de protection. Cette possibilité devrait toutefois constituer une exception au principe de base du maintien du secret. L'auteur de l'initiative fait valoir que ce nouveau régime met en danger la sécurité du droit dans les relations d'affaires courantes. Il demande par conséquent que l'autorité de protection des adultes soit tenue d'informer l'Office des poursuites du domicile de la personne concernée de toute mesure relevant du droit de la protection des adultes qu'elle prend ou qu'elle lève. En outre, l'Office des poursuites doit également être autorisé à retransmettre l'information.

Nous avons formulé les conditions qui doivent être remplies pour qu'un traitement de ces données soit conforme aux exigences de la protection des données. À notre avis, seules des informations relatives à la capacité contractuelle d'une personne peuvent être enregistrées. Les offices des poursuites ne sont à leur tour pas autorisés à transmettre ces informations sans preuve d'un intérêt particulier (tel que des négociations contractuelles); les communications de données à des sociétés de renseignements commerciaux doivent être clairement réglementées par la loi.

1.3 Internet et télécommunication

1.3.1 Les bourses d'échange sur Internet et le droit d'auteur – Situation actuelle

L'arrêt du Tribunal fédéral en la cause Logistep a créé une certaine incertitude en ce qui concerne la poursuite des violations des droits d'auteur sur Internet. C'est pourquoi la conseillère fédérale Simonetta Sommaruga a chargé un groupe de travail d'étudier les possibilités d'adapter le droit d'auteur à l'évolution technique. Son rapport final est disponible depuis début décembre 2013.

Suite à l'arrêt Logistep, il est devenu incertain s'il est encore possible, selon la loi en vigueur, de poursuivre les violations de droits d'auteur sur Internet. Alors que les ministères publics interprètent l'arrêt dans le sens que l'acquisition d'adresses IP sur Internet dans le but de poursuivre des violations du droit d'auteur est de manière générale illégale, nous sommes d'avis que l'acquisition et le traitement de telles données restent possibles, pour autant que certains principes sont respectés (cf. notre 20e rapport d'activités 2012/2013, ch. 1.3.3) Nous attendons toujours une clarification venant de la plus haute instance judiciaire.

Entre-temps, le groupe de travail AGUR12, institué par la conseillère fédérale Simonetta Sommaruga, a publié dans son rapport final ses propositions pour d'éventuels ajustements du droit d'auteur à l'évolution technique (disponible sur le site www.ige.ch, sous la rubrique Droit d'auteur – AGUR12). Le rapport renvoie directement à nos meilleures pratiques concernant la démarche à suivre lors de la collecte et du traitement de données personnelles à des fins de poursuite des violations du droit d'auteur sur Internet (cf. notre 19e rapport d'activités 2011/2012, ch. 1.3.7) et demande la création, si nécessaire, des bases légales appropriées. Nous saluons cette exigence et continuerons à suivre de près les évolutions dans ce domaine.

1.3.2 Explications concernant le webtracking

Les exploitants de sites web et la branche publicitaire recourent au traçage des utilisateurs (webtracking) afin de mieux positionner leurs offres sur Internet et se procurer un avantage sur leurs concurrents. La plupart du temps, les internautes ne s'en rendent pas compte. Du point de vue de la protection des données, le webtracking viole en règle générale les droits de la personnalité des personnes concernées et est donc illicite.

Les instruments de webtracking offrent de nombreuses possibilités: ils permettent par exemple d'analyser un site web ou de personnaliser la publicité, et sont également utilisés en relation avec des «plugins sociaux».

La fonction principale du webtracking consiste à enregistrer les activités des visiteurs sur un site web ou le comportement de navigation des internautes. Les données ainsi collectées permettent de tirer des conclusions quant à leurs intérêts, préférences ou habitudes. Selon le comportement de navigation, ceci permet de créer très rapidement des profils d'utilisateurs détaillés.

Nombre de ces instruments de webtracking posent problème du point de vue de la protection des données. Bien que l'enregistrement et l'analyse à proprement parler des données sont dans la plupart des cas effectués en toute discrétion par le fournisseur du service de webtracking, l'exploitant du site web porte sa part de responsabilité. Il intègre en effet à son site le code permettant le traçage des utilisateurs et favorise ainsi, à l'insu de l'internaute, la transmission de données, l'installation de cookies et la collecte de données.

Un principe important du point de vue de la protection des données pour l'exploitant du site web lors de l'utilisation du webtracking est le principe de la transparence: cela signifie que l'exploitant du site web doit informer en détail les visiteurs du fait qu'il utilise des outils de webtracking. Cette information peut par exemple se faire au moyen d'une déclaration de protection des données. Cette déclaration doit également mentionner les possibilités qu'a un visiteur de s'opposer au tracking.

Étant donné que le webtracking est généralement utilisé pour créer des profils de la personnalité, ceci requiert le consentement explicite du visiteur du site avant de pouvoir collecter des données – par exemple en lui demandant de donner son consentement par un clic de souris. Si le site web intègre des plugins sociaux, il est préférable qu'il propose une solution dite «à deux clics» qui permet au visiteur du site d'activer les plugins sociaux initialement désactivés pour ensuite partager la page avec d'autres utilisateurs.

De son côté, l'internaute a également diverses possibilités de se protéger contre le traçage. Comme première mesure, il est recommandé de supprimer après chaque session les cookies enregistrés et l'historique de navigation. De plus, de nombreux navigateurs sont munis d'une fonction paramétrable «Do not track» qui permet de signaler à la page affichée que l'on ne souhaite pas être soumis au webtracking.

De plus amples informations sur ce thème se trouvent sur notre site web www.leprepose.ch, dans la rubrique Protection des données – Internet et ordinateur.

1.3.3 Ordonnances concernant la loi sur les télécommunications

Dans le cadre de la consultation des offices, nous nous sommes prononcés sur les projets d'ordonnances relatives à la loi sur les télécommunications. Nous avons en particulier critiqué les données accrues exigées pour l'identification dans le domaine de l'enregistrement des noms de domaine, d'autant plus que ces données sont aussi enregistrées à l'étranger.

Nous avons été conviés à prendre position sur les ordonnances relatives au droit sur les télécommunications. Nous avons critiqué à cette occasion le nombre important de nouvelles données et surtout de documents exigés pour l'enregistrement de noms de domaines. Dans les commentaires explicatifs, il n'est pas précisé dans quelle mesure les exigences accrues concernant l'identification sont nécessaires et de ce fait proportionnées. Nous estimons que le renforcement de la sécurité des données est une conséquence de ces nouvelles exigences (en particulier lors du dépôt, de l'accès et de la sauvegarde). Si l'on considère que plusieurs bureaux d'enregistrement existent au niveau mondial pour les domaines «.ch» et «.swiss», les documents demandés pour l'identification devront alors être transférés aussi à l'étranger pour y être traités, et surtout pour y être stockés. L'accès des autorités à ces données qui seront traitées par des entreprises domiciliées à l'étranger est régi par le droit national correspondant et non par le droit suisse. Il en va de même de la surveillance du traitement des données effectué par les bureaux d'enregistrement.

1.3.4 Rapport du Conseil fédéral concernant l'ouverture des données publiques (Open data)

Dans le cadre de la consultation des offices, nous avons pris position sur le projet de rapport du Conseil fédéral en réponse au postulat Wasserfallen «Le libre accès aux données publiques comme priorité stratégique de la cyberadministration» et souligné, entre autres, les risques associés à une mise en relation des données.

Dans notre prise de position, nous avons attiré l'attention sur le risque que des données qui sont aujourd'hui anonymes en soi pourraient perdre leur anonymat si elles sont plus tard mises en relation avec d'autres données. Afin de contrer ce problème, il est mentionné à juste titre que les données doivent être régulièrement soumises à une vérification de leur conformité avec les exigences de la protection des données. De plus, la publication de données devrait être appliquée de manière restrictive, en y renonçant en cas de doute. Dans la pratique, on veillera à éviter les mises en relation abusives de données à l'aide de règles et procédures internes à l'administration.

1.3.5 Droit à l'oubli dans le cadre des archives numérisées des journaux

L'archivage numérique des journaux soulève de nombreuses questions du point de vue de la protection des données. Le «droit à l'oubli» a toujours existé mais est remis au goût du jour avec le développement des nouvelles technologies. Nous recevons régulièrement des questions sur ce thème et avons publié des explications sur notre site web.

Nous avons notamment été interpelés par une association de journalistes au sujet du «droit à l'oubli» dans le cadre des archives numérisées des journaux. De nombreux journaux ont en effet entrepris de numériser leurs archives et ceci pose de nombreuses questions du point de vue de la protection des données.

L'archivage numérisé d'articles journalistiques constitue un traitement de données personnelles au sens de la loi fédérale sur la protection des données (LPD). En cas d'atteinte à la personnalité, le traitement de données doit être légitimé par un motif justificatif, en principe par un intérêt public prépondérant. Il s'agit donc essentiellement d'une question de proportionnalité. Le principe de proportionnalité requiert que les données personnelles doivent être effacées ou être rendues anonymes après un certain délai, dans la mesure où leur conservation n'est plus justifiée. Il convient par conséquent de procéder à une pesée des intérêts et de mettre en balance, d'une part, l'intérêt de l'individu à l'effacement de ses données personnelles des archives numériques d'un journal ou de son intérêt au retrait de l'indexation dans les moteurs de recherche, d'autre part, l'intérêt public à la conservation des données dans les archives numériques ou dans les moteurs de recherche. Dans le cadre d'un litige, il appartient au juge, saisi d'une action civile fondée sur l'article 15 LPD ou sur l'article 28 du Code civil, d'effectuer cette pesée d'intérêts.

Nous suivons les développements de la mise en œuvre du «droit à l'oubli», notamment au niveau européen, et avons publié des explications sur ce thème sur notre site www.leprepose.ch, sous Protection des données – Internet.

1.3.6 Révision de la loi sur les publications officielles

Dans le cadre de la consultation des offices, nous avons exprimé notre avis sur la révision de la loi sur les publications officielles ainsi que sur les risques liés aux publications électroniques.

La loi sur les publications officielles (LPubl) règle la publication des recueils du droit fédéral (recueil officiel et recueil systématique) et de la Feuille fédérale. Dans le

cadre de la consultation des offices, nous avons pris position sur la révision de cette loi. Celle-ci prévoit un changement de primauté, c'est-à-dire le passage du caractère déterminant de la forme imprimée à la publication officielle sous forme électronique. Nous nous sommes en particulier engagés pour que les dispositions d'exécution de la LPubl prévoient des mesures permettant d'éviter les abus rendus possibles par les publications électroniques sur Internet (tels que la création de profils de la personnalité). Ces mesures devraient pouvoir être adaptées en permanence aux possibilités et développements techniques.

1.4 Justice/Police/Sécurité

1.4.1 Mise en œuvre Schengen: évaluation de la protection des données au Royaume-Uni

Nous avons, en octobre 2013, participé pour la deuxième fois à une évaluation Schengen dans le domaine de la protection des données. Une petite équipe d'experts a évalué la protection des données au Royaume-Uni. Les expériences qui y ont été faites ont été prises en compte pour l'évaluation de la Suisse en mai 2014.

C'est la deuxième fois que nous avons participé à une évaluation Schengen dans le domaine de la protection des données. Le tour du Royaume-Uni était fixé du 21 au 24 octobre 2013. Celui-ci avait été évalué pour la première fois en 2004 et avait alors fait l'objet de diverses recommandations.

Lors de cette évaluation, le comité d'évaluation était composé de six personnes, dont une collaboratrice du PFPDT comme représentante de la Suisse. Préalablement à l'évaluation, le Royaume-Uni avait dû répondre à un questionnaire et livrer divers documents. Le contrôle sur place a été effectué auprès des autorités de protection des données ainsi qu'auprès des autorités policières. Le rapport d'évaluation qui en résulte fait le point sur l'application des recommandations antérieures, sur l'indépendance et les activités de l'autorité de protection des données, sur l'application des droits de protection des données des personnes concernées et de la sécurité des données dans le cadre des «affaires Schengen» et émet des recommandations envers le Royaume-Uni.

Après avoir fait l'objet d'une consolidation entre les divers experts, le rapport a été soumis au Royaume-Uni pour consultation, avant d'être finalement présenté au groupe de travail du Conseil responsable des évaluations Schengen (SCHEVAL) au mois de décembre 2013, où il a été discuté et adopté. L'évaluation fait toujours l'objet d'un suivi au cours duquel l'État concerné peut démontrer dans quelle mesure il a pu appliquer les recommandations.

La Suisse a quant à elle été évaluée une première fois en 2008. Les expériences que nous avons faites en l'espèce ont été prises en compte pour la prochaine évaluation qui aura lieu en mai 2014.

1.4.2 Contrôle auprès du Consulat général de Suisse à Dubaï

Dans le cadre de la mise en œuvre des accords d'association à Schengen, nous avons mené un cinquième contrôle auprès d'une représentation suisse à l'étranger relatif aux traitements de données dans la procédure d'attribution des visas Schengen. En raison du nombre important de visas émis et de l'introduction des visas biométriques depuis octobre 2012, nous avons choisi le Consulat général de Suisse à Dubaï pour ce contrôle. À titre informatif, nous avons visité les locaux de l'entreprise auprès de laquelle le Consulat a externalisé une partie de la procédure.

Après les contrôles auprès des représentations suisses au Caire, à Kiev, Istanbul et Moscou, nous avons mené un contrôle relatif au traitement des demandes visas auprès du Consulat général de Suisse à Dubaï. Le contrôle a été annoncé auprès du Consulat en août 2013 puis, après réception et examen de la documentation demandée, un contrôle sur place a eu lieu en novembre 2013. L'ensemble du processus de contrôle s'est déroulé en collaboration étroite avec le conseiller à la protection des données du DFAE. Le Consulat de Dubaï a émis environ 19 000 visas en 2013 pour les résidents de Dubaï, de Oman et du Bahreïn. Les demandeurs qui se présentent au Consulat sont de nationalités très diverses en raison de l'importante immigration que connaît l'émirat.

Lors du contrôle sur place, nous avons visité les locaux du Consulat mais également les locaux de l'entreprise auprès de laquelle une partie de la procédure de traitement est externalisée, ces derniers étant situés sur le même étage que le Consulat. En effet, le Consulat sous-traite la première partie du processus, c'est-à-dire la prise de rendez-vous pour le dépôt des demandes ainsi que la vérification des dossiers de demande. Les collaborateurs de l'entreprise externe examinent donc le contenu des dossiers des demandeurs de visas et s'assurent que la totalité des informations et des documents requis s'y trouvent. Ce premier tri permet au Consulat de ne recevoir les demandeurs que lorsque leur demande est complète et d'optimiser de ce fait la procédure d'attribution.

La réception des dossiers, la capture des empreintes biométriques (visage et empreintes digitales), l'encaissement de la taxe puis l'analyse du dossier de demande qui débouche sur l'attribution ou non d'un visa et enfin le retour des passeports sont des tâches effectuées exclusivement par le Consulat au moment de notre contrôle. Depuis le mois de mars 2014, une plus grande partie de la procédure est externalisée: le Consulat ne traite plus directement avec les demandeurs mais se charge exclusivement de l'analyse des dossiers, de l'attribution et de l'émission des visas.

Parallèlement à la visite relative au contrôle, nous avons eu la possibilité de nous rendre dans les locaux de l'entreprise externe où sont accueillis les demandeurs depuis le mois de mars. Ces locaux sont situés à Dubaï également, mais pas dans le même bâtiment que le Consulat. Même si cette visite ne s'inscrivait pas dans le cadre du contrôle, elle nous a permis de nous rendre compte des conditions de traitement des demandes et des mesures mises en œuvre pour assurer la sécurité des données personnelles.

La documentation fournie par le Consulat (en particulier les directives internes en matière de traitement des demandes de visas) ainsi que la visite sur place nous ont permis de comprendre et d'analyser les traitements de données effectués par le Consulat. Nous avons pu constater que les mesures mises en œuvre pour assurer la sécurité des données étaient proportionnelles et adéquates par rapport à la sensibilité des données traitées, en particulier les données biométriques.

1.4.3 Projet d'externalisation du DFAE dans le cadre de la délivrance de visas Schengen

Diverses représentations suisses à l'étranger coopèrent avec des fournisseurs de services externes pour la délivrance de visas Schengen. Le DFAE prévoit d'étendre cette coopération. Nous avons examiné les projets de contrats et proposé des modifications, que le DFAE a acceptées.

Diverses représentations suisses à l'étranger collaborent avec des prestataires externes pour la délivrance de visas Schengen (cf. notre 19e rapport d'activités 2011/2012, ch. 1.4.1). Le Département fédéral des affaires étrangères (DFAE) souhaite maintenant étendre cette coopération. Ainsi, il prévoit d'externaliser non seulement la gestion des rendez-vous, mais aussi d'autres tâches, telles que la constitution de dossiers et la collecte de données biométriques. Dans ce contexte, nous avons demandé au DFAE de nous soumettre les projets de contrats concernés pour examen.

Nous avons examiné les projets de contrats quant à leur conformité avec la protection des données et avons en particulier vérifié qu'ils contiennent les dispositions du Code européen des visas, qui régit en détail la coopération avec des prestataires de services externes. Les projets de contrats contenaient l'essentiel des points pertinents de la législation sur la protection des données. Nous avons cependant demandé au DFAE de compléter divers points dans les contrats. Le DFAE nous a informés qu'il tiendrait compte de nos remarques dans les versions définitives de ses contrats.

1.4.4 Projet de loi sur le renseignement

Le projet de loi sur le renseignement transmis au Parlement contient des éléments problématiques du point de vue de la protection des données: l'utilisation d'aéronefs ou de satellites sans autorisation spécifique, la possibilité de s'introduire dans des systèmes et des réseaux informatiques et la non-application de la loi sur la transparence aux documents relatifs à la recherche d'informations au sens de la loi sur le renseignement.

Nous avons indiqué plusieurs fois que le projet de loi sur le renseignement n'est pas totalement satisfaisant du point de vue de la protection des données (cf. notre 20e rapport d'activités 2012/2013, ch. 1.4.6). Nous mentionnons ci-dessous les trois éléments les plus problématiques:

- Le projet prévoit la possibilité d'utiliser des aéronefs ou des satellites pour procéder à des observations dans des lieux publics ou dans des lieux librement accessibles. Une telle utilisation engendre automatiquement l'observation et l'enregistrement visuel et sonore de faits relevant de la sphère privée protégée. Pour cette raison et en tenant compte des événements récents en matière de surveillance au niveau international et de la difficulté à délimiter clairement l'utilisation de tels moyens, il convient de se demander si une telle utilisation ne devrait pas être ajoutée à la liste des mesures de recherche soumises à autorisation.
- Le projet prévoit également en plus des mesures de recherche d'informations, la possibilité de s'introduire dans des systèmes et des réseaux informatiques afin de perturber, empêcher ou ralentir l'accès à des informations. Nous sommes d'avis que ces moyens ne sont pas proportionnés. De telles mesures portent gravement atteinte aux droits fondamentaux et dépassent largement celles octroyées aux autorités de poursuite pénale.
- Nous sommes opposés à l'exclusion de l'application de la loi sur la transparence aux documents relatifs à la recherche d'informations au sens de la loi sur le renseignement (pour plus de détails cf. chiffre 2.5.1 du présent rapport d'activités).

Nous défendrons notre position dans le cadre des travaux des commissions parlementaires.

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

Au cours de l'année sous revue, nous avons pris position devant la Commission des affaires juridiques du Conseil des États 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.

Au cours du second semestre 2013, nous avons été invités par la Commission des affaires juridiques du Conseil des États 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).

Dans ce contexte, la Commission nous a priés de nous prononcer au sujet de l'arrêt du Tribunal fédéral du 22 janvier 2013 concernant la remise de données secondaires obtenues au cours d'une surveillance rétroactive. À notre avis, les fournisseurs de services de télécommunication ne doivent pas conserver les données secondaires au-delà des six mois requis par la LSCPT sans autre justification (par ex. une redevance due). Ils doivent donc configurer leurs systèmes de gestion de façon à ce que les données secondaires et les données relatives au trafic qui ne sont plus nécessaires soient effacées automatiquement. Dans le cas contraire, les autorités de poursuite pénale ont, selon le Tribunal fédéral, la possibilité de demander les données non effacées.

1.4.6 Communication de données personnelles aux autorités de police

Une association de quartier peut communiquer des données personnelles aux autorités de police, pour autant qu'elle respecte les principes généraux de protection des données.

Nous avons effectué un établissement des faits auprès d'une association de quartier, qui reçoit de ses membres, ou d'autres personnes, des informations sur des faits divers survenus dans le quartier (tels que trafic de drogue, incivilités,

parcages sauvages, problèmes de voisinage, etc.). Elle procède à un tri et les informations jugées pertinentes sont communiquées aux autorités de police compétentes. L'association ne conserve aucune donnée personnelle concernant ces évènements: tous les courriers électroniques, transmis ou non à la police, sont effacés, et l'association n'établit pas non plus de note concernant les appels téléphoniques ou les informations transmises de vive voix. Les signalements transmis par l'association sont traités par les autorités de police comme tout autre signalement arrivant à la centrale.

L'association nous a demandé si les traitements qu'elle effectue respecte la législation sur la protection des données. Comme une partie d'entre eux concerne des organes cantonaux et communaux, le préposé cantonal compétent a également participé à une séance avec l'association et la police communale.

Sur la base des éléments susmentionnés, nous avons ainsi constaté que l'association collecte des données personnelles; dans tous les cas, les noms des personnes qui signalent les faits, dans certains cas, des données concernant les «suspects»: noms, numéro de plaques, description, etc. L'association procède ensuite au tri des évènements signalés et finalement communique des données personnelles aux autorités de police.

Les annonces jugées pertinentes sont transmises aux autorités de police et sont ensuite détruites tandis que les annonces jugées non pertinentes sont détruites, de sorte qu'il n'y a pas de constitution de fichier. L'association informe les personnes qui font des annonces que celles-ci seront triées et que, en cas de communication aux autorité de police, leurs noms seront également transmis.

Nous sommes, sur la base des renseignements fournis, arrivés à la conclusion que la collecte, par l'association de quartier, d'informations relatives à une possible infraction puis leur communication à la police étaient dans le cas d'espèce conformes à la législation fédérale sur la protection des données.

1.4.7 Systèmes d'information de l'Administration fédérale des douanes

Dans le cadre des projets de révision de la loi sur les douanes et de deux ordonnances relatives aux systèmes d'information de l'Administration fédérale des douanes, nous avons une nouvelle fois indiqué que, conformément à la loi sur la protection des données, les organes fédéraux ne sont en droit de traiter et de communiquer des données personnelles que s'il existe une base légale.

Une base légale au sens formel est même exigée s'il s'agit de données sensibles ou de profils de la personnalité. La loi au sens formel doit régler en particulier plusieurs

points: les finalités de chaque système d'information doivent être définies de manière précise et reconnaissable pour les personnes concernées; l'organe fédéral responsable du traitement (maître de fichier) doit être mentionné; les participants à chaque système d'information doivent être reconnaissables; les catégories de données traitées doivent être définies, en particulier les catégories de données sensibles et les profils de la personnalité; les éventuelles restrictions au droit d'accès des personnes concernées doivent être mentionnées; l'architecture des systèmes informatiques doit être décrite dans les grandes lignes; la base légale doit définir l'organe fédéral compétent pour accorder l'accès en ligne, les autorités auxquelles un tel accès peut être accordé, les catégories de données accessibles et la finalité de l'accès.

À notre avis, les dispositions de la loi sur les douanes relatives aux systèmes d'information ne répondent pas à toutes les exigences mentionnées ci-dessus. Pour cette raison, nous avons proposé l'élaboration d'une loi sur les systèmes d'information des douanes comme c'est le cas dans les domaines de l'armée (loi sur les systèmes d'information de l'armée) et de la police (loi sur les systèmes d'information de police de la Confédération).

Dans le cadre de la préparation du message relatif à la révision partielle de la loi sur les douanes qui doit être remis au Conseil fédéral à fin 2014, le Département fédéral des finances est chargé de vérifier si les dispositions relatives aux systèmes d'information répondent aux exigences de la protection des données. Nous rappellerons notre position lors de la consultation des offices.

1.4.8 Révision totale de l'Ordonnance Interpol

Afin de tenir compte des changements intervenus dans deux règlements d'Interpol, l'Ordonnance Interpol suisse a été adaptée.

À la suite de développements techniques et organisationnels, les dispositions relatives au traitement de données de deux règlements d'Interpol ont été adaptées. Elles sont maintenant contenues dans un seul règlement. Ces adaptations ont nécessité la modification de la majorité des dispositions de l'ordonnance Interpol suisse. Pour cette raison, la révision est qualifiée de totale. Par contre, du point de vue matériel, les changements sont minimes. Dans le cadre de la consultation des offices, nous avons proposé quelques améliorations. L'Office fédéral de la police a tenu entièrement compte de nos remarques et nous a également présenté, lors d'une séance, les changements intervenus dans le domaine de l'échange d'informations dans le cadre d'Interpol.

1.4.9 Groupe d'experts FOGIS – Projet de loi sur la sécurité de l'information

Dans le cadre du groupe d'experts FOGIS, nous accompagnons le projet de loi sur la sécurité de l'information et veillons à la prise en compte des aspects liés à la protection des données et à la transparence.

Le Conseil fédéral a décidé en mai 2010 de modifier l'ordonnance sur la protection de l'information (OPrI) et de charger le DDPS de constituer un groupe de travail interdépartemental afin d'établir un projet de loi sur la sécurité de l'information. Celui-ci doit étendre les actuelles exigences en matière de protection de l'information aux mesures pour l'amélioration de la sécurité de l'information décidées le 16 décembre 2009 par le Conseil fédéral.

Ces mesures comportent également par nature des aspects liés à la protection des données (principe de sécurité), celle-ci étant elle-même conditionnée par des exigences de la transparence administrative. C'est dans ce contexte pluri- et interdisciplinaire qu'une vingtaine d'experts juridiques et techniques de plusieurs départements fédéraux se sont réunis à de nombreuses reprises sous la conduite du professeur Markus Müller de l'université de Berne (Groupe d'experts FOGIS).

Du point de vue formel, ce projet de loi désormais bien avancé doit encore faire l'objet de différentes procédures de consultation.

Du point de vue matériel, le projet de loi comporte six chapitres: dispositions générales, mesures générales de la sécurité de l'information, contrôles de sécurité relatifs aux personnes, procédures de sécurité industrielle, sécurité de l'information pour les infrastructures critiques, et organisation et exécution. Dans le chapitre consacré aux mesures générales, on trouve une section portant sur la classification de l'information en deux ou trois niveaux de sensibilité: secret, confidentiel ou interne.

Pour des raisons de facilité et clarté de mise en œuvre, nous soutenons le modèle à deux niveaux, tout en comprenant les arguments, notamment de compatibilité internationale, qui sous-tendent un modèle à trois niveaux. Par ailleurs, une analogie quant aux mesures de sécurité adéquates pourrait être établie avec les catégories de données personnelles respectivement les données «hypersensibles» (de nature à mettre en danger la vie ou l'intégrité corporelle), sensibles et non sensibles (selon la définition de la LPD)

Dans le chapitre consacré à l'organisation et à l'exécution, il est notamment prévu des préposés à la sécurité de l'information des autorités et des organisations concernées. Ceux-ci ont des tâches de conseil et soutien, de gestion de la sécurité et des risques selon le développement technique, ainsi que de contrôle du respect

des prescriptions. Une conférence de ces préposés à la sécurité de l'information permettrait d'assurer une certaine uniformité de l'exécution, un échange d'informations et d'expériences, ainsi que la nécessaire coordination avec d'autres organes concernés par la sécurité de l'information, en particulier le PFPDT. Enfin, un bureau/service fédéral pour la sécurité de l'information, sous la conduite d'un préposé fédéral à la sécurité de l'information, verrait le jour pour assurer la bonne exécution de cette loi, la collaboration nationale et internationale, de même que pour faire régulièrement un rapport de situation au Conseil fédéral.

Nous poursuivons nos travaux d'accompagnement de ce projet de loi et veillons à ce que les aspects liés à la protection des données et à la transparence soient pris en compte.

1.5 Santé et recherche

1.5.1 Projet de loi fédérale sur le dossier électronique du patient

La loi fédérale sur le dossier électronique du patient constitue la base légale nécessaire à la mise en œuvre de la cybersanté. Le projet actuel prend en compte d'importantes préoccupations de la protection des données. Pour l'identification du patient, il est prévu d'utiliser un identificateur sectoriel à la place du numéro d'assurance sociale. De plus, le patient doit avoir la possibilité de décider du contenu de son dossier électronique, des droits d'accès et de la confidentialité des informations médicales.

Le projet actuel de la loi fédérale sur le dossier électronique du patient (LDEIP) a pris en compte plusieurs préoccupations importantes de la protection des données. Suite nos interventions et au travail de persuasion que nous avons fourni il n'est ainsi plus prévu d'utiliser le numéro d'assurance sociale comme identificateur de patient dans le domaine de la cybersanté. Il est au contraire prévu d'utiliser comme identifiant du patient un numéro aléatoire, généré et géré par la Centrale de compensation (CdC). Ceci devrait permettre une identification sans équivoque du patient ou de la patiente ainsi qu'une attribution univoque des données du patient. Nous avons ainsi atteint un objectif important du point de vue de la protection des données. Nous avons également réussi à démontrer qu'il est possible d'utiliser des identificateurs sectoriels sans que leur introduction n'entraîne de frais supplémentaires excessifs.

En outre, il est également clair que le dossier médical électronique sera facultatif pour le patient ou la patiente. Il ne pourra être constitué que si la personne concernée a donné son consentement explicite après une information adéquate. Une fois qu'un dossier électronique a été ouvert, on présumera cependant que le patient ou la patiente accepte que les professionnels de la santé y saisissent des données lors des traitements médicaux. Il est important que le patient puisse ensuite décider de manière concrète, à l'aide des droits d'accès et des niveaux de confidentialité qu'il peut paramétrer, qui aura accès aux informations médicales sensibles. Ainsi, il est aussi prévu que certains professionnels de la santé puissent de manière générale être privés de droit d'accès. Nous pouvons donc constater que le projet dans sa forme actuelle tient compte dans son orientation générale de nos préoccupations.

Quelques questions importantes telles que la procédure de certification des communautés de cybersanté, les exigences envers l'identité électronique des patients et patientes ainsi que des professionnels de la santé, de même que les services de consultation exploités par l'Office fédéral de la santé publique ne seront cependant concrétisées que dans le cadre des dispositions d'exécution.

1.5.2 Compétence du PFPDT en matière de protection des données dans les hôpitaux

Le partage de compétences entre les autorités cantonales de protection des données et le PFPDT n'est pas toujours évident pour les personnes concernées. Nous avions jusqu'ici considéré que nous étions compétents pour les hôpitaux privés. Cette compétence est pourtant mise en doute actuellement par une expertise mandatée par l'Association des commissaires suisses à la protection des données (privatim).

Une expertise mandatée par privatim conclut qu'un hôpital est soumis au contrôle de l'autorité de surveillance cantonale s'il fournit des prestations sur mandat du canton, ceci indépendamment de sa forme juridique. C'est le cas lorsqu'un hôpital figure sur une liste des hôpitaux cantonaux et qu'il fournit les prestations ou services suivants:

- prestations stationnaires de l'assurance obligatoire des soins (AOS);
- prestations stationnaires pour d'autres assurances sociales (assurance-invalidité, assurance-accidents, assurance militaire), dans le cas de mandats soumis au droit cantonal;
- prestations ambulatoires, dans le cas de mandats soumis au droit cantonal;
- prestations du domaine de l'assurance complémentaire, au cas où une contribution de base de l'assurance obligatoire est due;
- prestations d'enseignement et de recherche, dans la mesure où elles sont couvertes par des mandats de prestations soumis au droit cantonal (p.ex. dans le domaine de l'enseignement et de la recherche universitaire);
- prestations d'urgence fournies dans le cadre de mandats de prestations.

De plus, la compétence d'une autorité cantonale de surveillance en matière de protection des données doit également s'étendre aux hôpitaux extracantonaux pour le domaine des prestations AOS stationnaires, dans la mesure où ces derniers exécutent des mandats de prestations pour le canton concerné. L'expertise relève également que les hôpitaux agissent selon les principes de l'économie privée lorsqu'ils ne remplissent pas des mandats de prestations cantonaux et sont donc dans ces cas soumis à la surveillance du PFPDT, à moins qu'une disposition cantonale ne prévoie expressément une autre compétence.

Si l'on suivait la conclusion de cette expertise, cela signifierait que les hôpitaux remplissant aussi bien des tâches publiques que privées seraient soumis à deux autorités de surveillance distinctes et devraient appliquer différentes lois de

protection des données. L'auteur de l'expertise mentionne d'ailleurs que la situation est compliquée et confuse et doit être considérée comme insatisfaisante. Nous sommes d'avis que cette position peut en effet être très intéressante d'un point de vue juridique, mais qu'elle n'est pas raisonnablement praticable, ni pour les hôpitaux, ni pour les patients et patientes.

On ne peut pas exiger d'un patient qu'il fasse des recherches juridiques approfondies pour savoir quel droit de la protection des données est applicable à quel traitement médical et à quelle autorité de protection des données il peut s'adresser. Un groupe hospitalier privé ayant des hôpitaux dans plusieurs cantons ne devrait pas avoir à s'occuper de savoir quelle autorité de protection des données est compétente pour un patient donné ou qui est l'interlocuteur compétent pour un système hospitalier d'information centralisé, si ce dernier est par exemple exploité à Zurich, mais utilisé par tous les hôpitaux du groupe.

Dans ce sens, nous continuerons à conseiller les hôpitaux privés ainsi que les patients et patientes qui se sont fait soigner dans un hôpital privé. Nous continuerons également à assumer nos tâches de contrôle auprès des hôpitaux privés. Au cas où un hôpital privé devait mettre en doute notre compétence, ceci pourrait mener à une procédure judiciaire. Dans un tel cas, le tribunal saisi devrait clarifier la question du for compétent et du droit applicable.

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

Le Conseil fédéral a chargé le Département fédéral de l'intérieur d'élaborer un projet de loi sur l'enregistrement des maladies oncologiques et le message y relatif d'ici la fin de l'année. Lors de la consultation externe, nous avons rappelé les risques liés à l'utilisation du numéro AVS en tant qu'identifiant unique pour la sphère privée des personnes concernées.

Le Conseil fédéral entend créer une base légale afin de répertorier de manière complète et uniforme les données concernant les cancers:

La loi fédérale sur l'enregistrement des maladies oncologiques se basera sur le système décentralisé existant, tout en le complétant. Les données figurant dans les registres cantonaux seront transmises à un organe national d'enregistrement du cancer financé par la Confédération, qui sera chargé de les regrouper, de les évaluer et de les publier. Le financement des registres cantonaux et régionaux incombera toujours aux cantons. À l'avenir, un ensemble minimal de données, comprenant notamment le diagnostic précis, la date à laquelle il a été posé et celle à laquelle le traitement a débuté, sera collecté pour chaque cas. Pour certains cancers

spécifiques, des données complémentaires seront recensées (par exemple des informations relatives à l'évolution de la maladie ou du traitement).

Lors de la consultation externe, nous avons rappelé, conformément à nos précédentes prises de position (cf. notre 20e rapport d'activités 2012/2013, ch. 1.5.5), 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. Il faut en effet à tout prix éviter de mélanger les domaines de la statistique, de l'administration et de la santé, les exigences liées à ces domaines étant différentes aussi bien du point de vue de la quantité que de la qualité des données. L'utilisation d'un numéro spécifique à chaque domaine réduit 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.

Constatant que le projet maintient le numéro AVS en tant qu'identificateur, nous avons rappelé encore une fois la nécessité de mettre en place des alternatives à l'utilisation du numéro AVS, 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). Il ne s'agirait pas ici d'utiliser le même numéro sectoriel que le dossier patient mais un autre numéro spécifique aux registres du cancer.

Le 30 octobre 2013, le Conseil fédéral a pris connaissance du rapport relatif à la procédure de consultation externe. Si les participants ont largement plébiscité la création d'une règlementation au niveau fédéral, certains points demeurent toutefois controversés. Les prises de position diffèrent en ce qui concerne, par exemple le volume des données nécessaires pour évaluer la qualité du traitement et des soins. Ces questions seront encore traitées avec les acteurs concernés en vue de l'élaboration du message.

Par ailleurs, il y a lieu de remanier certains points relatifs aux droits des patients et à la protection des données. Cela concerne notamment l'information des patients et l'utilisation, par des tiers, des données collectées. Le Conseil fédéral a donc chargé le Département fédéral de l'intérieur d'élaborer le projet de loi et le message y relatif d'ici la fin de l'année. Pour notre part, nous veillerons à ce que nos réserves relatives à l'utilisation du numéro AVS soient prises en compte.

1.5.4 Changement de compétence pour l'octroi d'autorisations dans le domaine de la recherche médicale

Nous avons effectué plusieurs contrôles dans le domaine de la recherche médicale et avons relevé divers points qui n'ont pas encore été mis en œuvre de manière optimale. C'est surtout au niveau de la documentation des projets que des améliorations sont nécessaires. Les contrôles avaient également pour objectif de fournir aux commissions d'éthique des indications précieuses pour leur travail futur.

Nos contrôles ont permis de constater que, pour de nombreux projets de recherche, les processus n'étaient pas suffisamment documentés. Pour des raisons de transparence, ces processus jouent cependant un rôle important, aussi bien pour la recherche même que pour les organes qui délivrent les autorisations. La documentation doit mentionner les étapes essentielles, depuis la collecte des données personnelles non cryptées (non pseudonymisées) jusqu'à leur pseudonymisation, anonymisation ou suppression. Il est également important d'indiquer quel fichier sera utilisé pour le projet de recherche. Ce n'est qu'ainsi qu'il sera possible de vérifier si cet enregistrement est réellement anonyme. Il y a lieu, dans ce contexte, de noter que l'on traitera uniquement les données qui sont nécessaires pour le projet de recherche. Quant au cryptage ou à la pseudonymisation, on veillera à ce qu'il soit, dans la mesure du possible, effectué à l'endroit où les données ont été collectées. Ceci sera dans la plupart des cas auprès du médecin traitant. Ce n'est que sur la base de ces informations que l'on pourra se procurer une vue d'ensemble et évaluer la conformité du projet de recherche aux exigences de la protection des données.

En ce qui concerne le consentement, la loi relative à la recherche sur l'être humain (LRH) stipule nouvellement qu'en fonction de la situation ce dernier peut ou doit être obtenu non seulement de la personne concernée, mais aussi de son représentant légal ou de ses proches parents. Cette pratique est souhaitable, car elle permet d'obtenir un consentement dans la majorité des cas. Il convient en particulier de veiller à ce que les informations soient bien compréhensibles pour les personnes appelées à donner leur consentement. Il est indispensable de leur expliquer comment se déroule le projet de recherche et quelles sont les mesures de protection qui ont été prises. Si l'information n'est pas faite de manière transparente, ceci présente le risque que le consentement ne soit pas considéré comme valable.

L'article 34 LRH prévoit précisément les conditions auxquelles les traitements de données personnelles (ou d'échantillons biologiques) peuvent être effectués sans consentement ou sans indication relative au droit d'opposition. Reprenant la

formulation de l'ancien article 321bis CP, cette disposition stipule qu'un projet de recherche peut être réalisé si les trois conditions suivantes sont cumulativement remplies:

- l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées, ou on ne peut raisonnablement l'exiger de la personne concernée.
- aucun document n'atteste un refus de la personne concernée.
- l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données.

Lors de nos précédents contrôles des charges, nous avons constaté, que le droit de veto (ou droit d'opposition) n'était souvent pas connu des personnes concernées, malgré le fait que cette information était transmise par exemple dans les brochures destinées aux patients. Ce droit de veto vaut pour tous les projets de recherche. Cela signifie que les données ne peuvent pas être utilisées pour la recherche. La question se pose dans ce contexte de savoir où veto doit être consigné pour que tous les chercheurs sachent qu'ils ne peuvent pas utiliser ces données. Il serait par ailleurs nécessaire que les organes de contrôle puissent vérifier si une opposition existe.

1.6 Assurances

1.6.1 Contrôle des services de réception des données des assureurs-maladie pour les factures de type DRG

Le contrôle de deux services de réception des données déjà certifiés a révélé que la mise en œuvre du contrôle automatisé de vraisemblance des factures de type DRG progresse, pour des raisons techniques, moins rapidement que prévu.

Au cours de l'année sous revue, nous avons contrôlé les services de réception des données pour les factures de type DRG auprès de deux assureurs-maladie. Ces contrôles nous ont permis de constater que seule une très petite part des factures – comprenant toutes les informations nécessaires, en particulier les données médicales – étaient livrées aux services de réception des données sous forme électronique. La principale raison du retard de cette mise en œuvre est, selon nos observations, l'introduction tardive de l'enregistrement standardisé dans les systèmes que les hôpitaux utilisent pour l'établissement des factures.

Nous avons ainsi pu constater lors du contrôle du service de réception des données d'un grand assureur-maladie que ce dernier était prêt pour un contrôle automatisé de vraisemblance des factures DRG, mais qu'il ne pouvait l'utiliser que de manière limitée, en raison du grand nombre de factures reçues sous forme papier. Cet assureur a toutefois également fait certifier les processus et systèmes qui sont nécessaires pour le traitement des factures papier de type DRG. Cela signifie qu'il remplit les exigences envers un service de réception des données certifié.

Lors d'un autre contrôle auprès d'un assureur-maladie de taille moyenne, nous avons cependant constaté que ce dernier n'avait pas fait certifier ses processus pour le traitement des factures DRG papier, parce qu'il comptait sans doute sur une introduction en temps voulu du format électronique. Lors de notre contrôle, l'assureur pensait toujours renoncer à une certification des processus papier, étant donné qu'il prévoyait refuser les factures papier de type DRG à partir du 1er janvier 2014. Une des raisons était le fait que l'assureur collabore avec un prestataire externe pour l'exécution des contrôles de vraisemblance automatisé et que ce prestataire avait expressément déclaré – du moins au moment du contrôle – vouloir traiter uniquement des factures électroniques.

Il s'est avéré entre-temps que ces plans ont peu de chance de pouvoir être mis en œuvre, vu que même à fin 2013 la part des factures électroniques DRG se situait encore bien en dessous de 50 pour cent. À notre avis, il n'existe qu'une seule solution pour cet assureur ainsi que pour tous les autres qui ne l'ont pas déjà fait: faire certifier les processus papier des services de réception des données. À part

cela, nous n'avons pas été en mesure de vérifier la proportionnalité des factures transmises à l'assureur après le contrôle automatisé de vraisemblance, étant donné que le nombre de factures électroniques traitées par les SRD était, comme nous l'avons expliqué ci-dessus, trop faible.

1.6.2 Certification des services de réception des données

De nombreux assureurs-maladie ont fait certifier leurs services de réception des données et les ont annoncés chez nous. Les petits et moyens assureurs-maladie font souvent effectuer le contrôle automatisé de vraisemblance par un prestataire externe. Les groupes d'assureurs par contre préfèrent exploiter un service de réception des données central pour tous les membres du groupe.

Les assureurs recevant un certificat pour leur service de réception des données (SRD) doivent l'annoncer chez nous. Nous publions sur notre site (www.leprepose.ch, Protection des données – certification – SwissDRG) une liste des services de réception des données qui sont certifiés. Cette liste permet de voir si un assureur exploite lui-même un service de réception des données, si ce dernier travaille pour plusieurs assureurs d'un groupe, si un prestataire effectue le contrôle automatisé de vraisemblance, quel organe a délivré la certification et jusqu'à quand le certificat est valable. Jusqu'à janvier 2014, 39 SRD se sont annoncés chez nous.

Le nombre de ces annonces permet de tirer diverses conclusions. Les petits et moyens assureurs-maladie ont en majorité délégué le contrôle automatisé de vraisemblance à un prestataire externe. Actuellement, cette externalisation semble se concentrer sur deux prestataires. Certains assureurs-maladie de taille moyenne ont cependant décidé d'effectuer ce traitement eux-mêmes. Quant aux grands groupes d'assureurs, ils exploitent un SRD central pour leurs membres. De leur point de vue, ceci constitue à vrai dire une externalisation à la société du groupe.

Ce qui importe dans le cas d'une collaboration avec un prestataire est que tous les processus qui sont nécessaires pour l'exploitation du SRD aient été certifiés aussi bien auprès de l'assureur qui délègue qu'auprès du prestataire-même. Un prestataire ne peut donc jamais à lui seul obtenir un certificat pour son service de réception des données, étant donné que ce dernier est toujours établi pour un assureur ou un groupe donné. Dans les cas où le certificat est établi pour un groupe, il doit d'ailleurs mentionner clairement pour quels membres il est valide. Bien sûr, ceci doit ressortir tout aussi clairement du rapport d'audit correspondant.

Au cours de l'année sous revue, nous avons assisté une nouvelle fois à une réunion des organismes de certification accrédités: KPMG AG, l'Association Suisse pour Systèmes de Qualité et de Management (SQS) et le Service d'accréditation suisse

(SAS). Nous y avons en particulier parlé des exigences envers la formation des experts engagés dans les audits de certification, les exigences envers le rapport d'audit et la durée nécessaire de l'audit. Étant donné que la certification en matière de protection des données se base sur la norme ISO/IEC 27001, nous avons logiquement déclaré que la norme ISO/IEC 27006 valable pour les audits avait force obligatoire.

En outre, nous avons réitéré la précision explicite que nous avions déjà apportée lors de la séance en automne de l'année précédente, à savoir que les services de réception des données devaient également faire certifier leurs processus papier. À notre avis, ces séances de travail se sont avérées très utiles puisqu'elles nous permettent, en qualité de détenteur du schéma de certification, de discuter des problèmes et de trouver des solutions directement avec les organismes impliqués, mais aussi de transmettre et d'expliquer nos exigences qui sont contraignantes pour les organismes de certification. En conséquence, nous continuerons à organiser cette réunion chaque année. Si cela s'avère nécessaire, nous convoquerons également des réunions ad hoc.

1.6.3 Réduction individuelle des primes – Transmission de données d'assurés aux organes cantonaux

L'accord de réductions individuelles de prime va engendrer des communications de données de grande envergure des assureurs-maladie aux organes cantonaux d'exécution. Nous doutons que cette démarche soit admissible.

Dans le cadre de la réduction individuelle des primes (RIP), l'Office fédéral de la santé publique (OFSP) a fait modifier l'ordonnance sur l'assurance-maladie, donnant maintenant la possibilité aux cantons d'inclure dans leurs lois des dispositions qui permettent d'obliger les assureurs-maladie à mettre en place certains processus de communication de données. Nous défendons cependant clairement l'avis que seule une disposition de la loi fédérale peut être considérée comme base légale suffisante pour les assureurs de l'assurance obligatoire des soins (AOS), étant donné que ceux-ci agissent en tant qu'organes fédéraux.

Nous considérons comme particulièrement critique le processus de communication «effectif complet des assurés». Ce dernier demanderait aux assureurs-maladie de transmettre aux organes d'exécution cantonaux l'effectif complet des personnes qui sont assurées selon la loi sur l'assurance-maladie. Nous avons, dans plusieurs prises de position adressées à l'OFSP, qualifié ces communications de données comme étant disproportionnées, car elles contiennent également des données de personnes qui n'ont pas droit à une réduction de prime ou qui, pour une raison ou une autre, ne désirent pas faire valoir ce droit.

Certains assureurs-maladie, qui ne sont également pas convaincus de la licéité de ce processus, nous ont contactés en nous priant de prendre position. Nous avons clairement retenu qu'une disposition cantonale ne pouvait pas servir de base légale à une communication de données effectuée par un organe fédéral. De plus, le processus de communication «effectif complet des assurés» viole le principe de la proportionnalité, étant donné qu'il n'est pas nécessaire pour pouvoir accorder la RIP. Nous attendons maintenant de l'OFSP qu'il fasse rapidement créer une base légale claire pour les processus de communication effectués dans le cadre de la RIP, qui respecte également le principe fondamental de la proportionnalité.

1.7 Secteur du travail

1.7.1 Communication de données relatives à des collaborateurs par les banques – Nouveaux développements

Après avoir émis des recommandations à l'intention de cinq banques en 2012, nous avons, dans le cadre de la discussion concernant une solution globale au différend fiscal, élaboré un feuillet thématique expliquant la démarche à suivre pour les banques souhaitant communiquer des données personnelles dans le cadre de cette affaire. Nous avons en outre conseillé des personnes concernées et leur avons expliqué quels étaient leurs droits.

En automne 2012, nous avons, dans le cadre de la transmission de données de collaborateurs aux autorités américaines, procédé à un établissement des faits auprès de cinq banques. Nous avons conclu ces examens en octobre 2012 avec cinq recommandations. Au cours du débat ayant eu lieu au printemps 2013 au sujet d'une solution globale au différend fiscal avec les États-Unis, la discussion a porté sur des communications de données effectuées par d'autres banques. Nous avons à nouveau été contactés et avons participé à différentes réunions internes à l'administration. Nous y avons expliqué notre position ainsi que la procédure esquissée dans nos recommandations.

Nous avons souligné que même les banques n'appartenant pas au cercle des destinataires de nos recommandations doivent appliquer les principes de protection des données lors de la transmission de données personnelles aux autorités américaines et doivent donc dans ce sens s'en tenir à nos recommandations. Le Parlement n'ayant pas créé de base légale, nous avons publié un feuillet thématique. Ce dernier décrit la démarche que nous demandons de suivre avant toute communication de données personnelles. Elle s'adresse à toutes les banques qui sont concernées. Dans le même temps, nous nous sommes adressés par écrit à plusieurs banques, les informant de l'existence de ce feuillet thématique. Nous avons par ailleurs continué à conseiller des personnes concernées et à leur expliquer quels étaient leurs droits.

1.7.2 Établissement des faits en matière de lanceurs d'alertes (whistleblowing)

Dans le cadre d'un établissement des faits, nous avons examiné le traitement de données effectué sur des messages transmis au bureau de communication du Contrôle fédéral des finances et évalué sa conformité avec les exigences de la protection des données. Nous avons émis des recommandations concernant l'obligation de déclarer le fichier et l'élaboration d'un règlement de traitement.

Depuis 2003, le Contrôle fédéral des finances (CDF) dispose d'un bureau de communication auquel les collaborateurs de l'administration fédérale peuvent s'adresser s'ils constatent des irrégularités ou s'ils ont des soupçons de corruption. De plus, le 1er janvier 2011 est entré en vigueur un nouvel article de la loi sur le personnel de la Confédération qui stipule que les collaborateurs sont même, sous certaines conditions, obligés de signaler les irrégularités. Le bureau de communication nouvellement mis en place doit permettre d'une part de sanctionner les actes punissables (obligation d'annoncer), d'autre part de combattre la corruption (droit de dénoncer) et empêcher ainsi que les collaborateurs communiquent de telles informations d'abord à la presse.

Dans le cadre de notre activité de surveillance, nous avons examiné en 2013 la conformité avec les dispositions en matière de protection des données du traitement effectué auprès du bureau de communication pour lanceurs d'alerte. Dans un premier temps, nous avons remis au CDF un questionnaire. Puis nous avons effectué une inspection sur place avant de rédiger un rapport final sur la base de ces informations.

Le CDF traite des données personnelles au sens de la loi fédérale sur la protection des données (LPD), même si certaines dénonciations sont faites de manière anonyme. Les données sont stockées en interne au sein du CDF et traitées exclusivement par les personnes compétentes. Nos investigations nous ont menés à la conclusion que le CDF exploite un fichier. Selon la LPD, les organes fédéraux sont tenus de déclarer tous leurs fichiers au PFPDT et, en cas de traitement de données personnelles sensibles, ils doivent élaborer un règlement de traitement. Nous avons recommandé au CDF d'adapter son traitement de données en fonction de nos explications. Nos recommandations n'ayant pas été acceptées, la procédure est encore pendante.

1.7.3 Enregistrement des conversations téléphoniques auprès du service clientèle de la Poste

Nous avons ouvert une procédure d'éclaircissement des faits auprès de la Poste Suisse suite à la plainte d'un syndicat concernant les enregistrements téléphoniques des collaborateurs du service clientèle. L'issue du contrôle nous a permis de conclure que les prescriptions en matière de protection des données, notamment l'information aux collaborateurs et la proportionnalité des processus de contrôle, étaient respectées en l'espèce.

Un syndicat nous a fait part de ses préoccupations concernant les enregistrements téléphoniques des employés des centres d'appels de la Poste Suisse. Nous avons décidé l'ouverture d'une procédure d'éclaircissement des faits. Il s'agissait alors de déterminer de façon générale si les processus de traitement mis en place par la Poste Suisse respectaient la législation en matière de protection des données dans le cadre des enregistrements des appels téléphoniques de ses collaborateurs. En revanche, cette procédure ne portait pas sur la vérification de cas individuels. Cette approche relève en effet de la compétence d'un juge civil, lequel peut établir si des dispositions sur la protection de la personnalité ont été enfreintes dans un cas spécifique, c'est-à-dire à la demande d'un collaborateur s'estimant lésé.

L'issue du contrôle nous a permis de conclure que les prescriptions en matière de protection des données, notamment l'information aux collaborateurs et la proportionnalité des processus de contrôle, sont respectées en l'espèce. En effet, notre analyse a permis de mettre en évidence que seul un certain pourcentage d'appels fait l'objet d'enregistrements et seuls les appels enregistrés durant des périodes déterminées et annoncées préalablement aux collaborateurs concernés sont utilisés pour évaluer leurs prestations. Les autres appels enregistrés ne le sont qu'à des fins d'évaluation des processus métiers et non à des fins de contrôle des prestations des collaborateurs.

L'utilisation de ces données ne vise qu'à une amélioration générale des processus ou à l'identification d'un besoin global (et non individuel) de formation. Les enregistrements sont uniquement requis sur la base de critères généraux et transversaux et non selon l'identité des collaborateurs. L'évaluation des processus métiers et les enregistrements requis dans ce cadre ne servent pas à l'évaluation spécifique des collaborateurs. Ainsi, chaque employé reçoit une information sur le processus de surveillance des appels, non pas au moyen d'un signal acoustique ou optique, mais par une information préalable claire et transparente des périodes d'enregistrements qui lui sont notamment accessibles via le site intranet de l'entreprise.

De même, nous avons considéré que la durée des périodes d'enregistrements répond aux exigences de la protection des données dans la mesure où la fréquence des périodes et la durée des appels enregistrés respectent le principe de proportionnalité. L'enregistrement n'est ni constant ni systématique. En outre, la fonction d'écoute en temps réel des appels en cours par le supérieur hiérarchique est définitivement désactivée. L'accès aux enregistrements est limité à un nombre restreint de personnes qui en ont besoin pour effectuer leur tâche. La durée de conservation des données est également limitée dans une mesure proportionnée.

Cependant, en vue d'améliorer l'information transmise à ses employés, la Poste Suisse a, sur notre proposition, modifié ses instructions internes. Celles-ci distinguent plus clairement entre le processus visant l'amélioration de la qualité des prestations des collaborateurs d'une part et celui concernant l'amélioration des processus métiers d'autre part. Des précisions concernant les deux finalités d'un tel système, le cercle des personnes autorisées à écouter les appels, ainsi que les durées de conservation des données ont également été apportées et contribuent à une meilleure compréhension des instructions internes.

Les collaboratrices et collaborateurs du service clientèle disposent dès à présent de directives claires, leur permettant de déterminer à quelles conditions leur données peuvent faire l'objet d'un traitement de façon licite et dans le cas contraire entreprendre les démarches qu'ils estiment nécessaires à la défense de leurs droits. Ainsi, dans l'hypothèse où un collaborateur estime que les conditions d'enregistrement le concernant ne sont pas correctes, en particulier si elles ne respectent pas les instructions ou la législation sur la protection des données, il a la possibilité d'agir à titre individuel.

À noter que le contrôle susmentionné a porté sur les aspects de protection des données, à l'exclusion de ceux du droit du travail. Pour sa part, le Secrétariat d'État à l'économie (SECO) a édicté des commentaires sur la mise en œuvre de l'article 26 de l'ordonnance 3 relative à la loi sur le travail (OLT 3). Le contrôle de l'application de cette ordonnance, et partant de la manière selon laquelle est effectuée la surveillance des employés à des fins de formation, de contrôles de qualité ou de contrôle de performance, relève des inspections cantonales du travail.

1.7.4 Envoi de certificats de caisse de pension – Difficultés rencontrées dans la pratique

À l'occasion de notre contrôle auprès de AXA Winterthur concernée par l'arrêt du 10 avril 2012 du Tribunal administratif fédéral, nous avons pu constater que la caisse de pension avait modifié sa pratique conformément au jugement. Il apparaît néanmoins que d'autres acteurs de la prévoyance professionnelle n'ont pas encore changé leur pratique.

Dans son arrêt du 10 avril 2012, le Tribunal administratif fédéral (TAF) a posé des principes bienvenus en matière de transmission des données par les institutions de prévoyance suisses. Cet arrêt a notamment mis fin à la pratique, attentatoire aux droits de la personnalité des employés, qui consistait à transmettre – sous pli non fermé – les certificats de caisse de pension aux employeurs. Selon la jurisprudence désormais établie, les certificats doivent être remis de telle sorte que seule la personne assurée – à l'exclusion de tout tiers, notamment l'employeur – puisse prendre connaissance de leur contenu (cf. notre 20e rapport d'activités 2012/2013, ch. 1.7.2).

La notion de tiers a été centrale pour la résolution du problème. Bien que souvent utilisée dans la loi sur la protection des données (LPD), elle n'y est pas définie. Le TAF a dès lors clarifié la question à la lumière de la théorie de la fonction. Selon celle-ci, un tiers est toute personne qui, du point de vue de la nature de ses attributions au sein d'une entreprise, ne nécessite pas l'accès aux données personnelles en jeu pour accomplir ses tâches. L'exemple que donne le TAF pour illustrer ce cas est celui du chef de service qui prend connaissance, volontairement ou non, du dossier personnel d'un employé appartenant à un service différent.

Selon le TAF, cet état de fait est constitutif d'une communication de données à un tiers, quand bien même elle a lieu au sein de la même organisation. Une telle diffusion de l'information n'est légitime, du point de vue de la protection des données, qu'en présence d'un motif justificatif (à savoir la loi, le consentement, un intérêt prépondérant privé ou public), sans quoi la communication des données constitue une atteinte illicite à la personnalité de l'employé concerné.

En l'espèce, il a été retenu que les institutions de prévoyance professionnelle, indépendamment de leur forme juridique, remplissent des tâches publiques. Elles sont ainsi considérées comme des organes fédéraux lorsqu'elles accomplissent les obligations qui leur sont dévolues par la loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP). Ce constat est important, car suivant qu'un traitement est effectué par une entreprise privée ou l'administration publique, les dispositions applicables sont différentes.

En effet, le législateur a prévu des conditions plus restrictives en matière de traitements de données par les organes fédéraux. Seule une base légale peut justifier un traitement dans un cas pareil, contrairement aux privés qui bénéficient de plusieurs motifs justificatifs. En l'occurrence, le TAF a conclu qu'il n'existe aucune base légale permettant de déroger à l'obligation de garder le secret applicable en matière de prévoyance, et aucune justification de la communication des certificats aux employeurs ou à tout autre tiers ne peut ainsi être invoquée.

Rappelons de plus que les certificats des caisses de pension contiennent des informations qui dans les rapports de travail peuvent avoir une portée stratégique. On peut notamment y découvrir: les prestations de libre passage qu'apportent avec eux de nouveaux collaborateurs, les rachats d'années d'assurance, le prélèvement d'une partie de l'avoir pour l'acquisition d'un logement, si et quand l'avoir a changé suite à un divorce, les références à une éventuelle incapacité de travail temporaire, etc.; autant d'éléments qui peuvent être exploités à d'autres fins que celles de la prévoyance professionnelle.

L'institution doit par conséquent prendre toutes les mesures nécessaires pour garantir que les informations, parfois sensibles, de ses assurés ne soient pas divulguées lors de l'envoi. La sécurité des données doit être préservée, c'est un élément inhérent aux devoirs de diligence de l'institution de prévoyance. Concrètement, cela signifie que les certificats doivent être envoyés soit directement sous pli fermé à l'adresse privée des assurés, soit à l'employeur pour distribution dans une enveloppe cachetée portant le nom du destinataire et la mention «personnel».

Malgré une prise de position claire du TAF en la cause, des indications relatives à des manquements nous parviennent encore. Il convient de ce fait de rappeler que l'arrêt, bien qu'étant un acte individuel et concret ne concernant dans un premier temps que les parties au contentieux, constitue une précision du droit de la protection des données qui trouve une application générale et abstraite. La jurisprudence, ainsi développée, est par essence applicable à tous les acteurs concernés, favorisant simultanément la sécurité du droit.

Au vu de ce qui précède, nous continuerons de garder un œil attentif sur les développements futurs dans ce domaine.

1.7.5 Système d'information concernant le personnel de la Confédération

De grandes quantités de données personnelles sont traitées dans le système d'information concernant le personnel de la Confédération BV PLUS. Suite à diverses demandes et compte tenu du volume de données traitées, nous nous sommes fait expliquer ce système. Ceci nous a en même temps permis de comprendre les projets que nous avons examinés dans le cadre des consultations des offices.

L'année dernière, nous avons constaté une recrudescence de questions concernant le système central informatisé de gestion du personnel de la Confédération BV PLUS, aussi bien dans le cadre de notre activité de conseil que de l'accompagnement des projets législatifs et des consultations des offices. C'est pourquoi il était important pour nous d'apprendre à mieux connaître ce système. En sa qualité d'exploitant du système d'information, l'Office fédéral du personnel (OFPER) nous a expliqué les différents modes de fonctionnement de BV PLUS par le biais d'une présentation. Lors d'une réunion commune, nous avons en outre discuté de plusieurs projets futurs et de questions de détail.

En 2013, nous avons également accompagné d'autres projets législatifs qui impliquaient des données en provenance de BV PLUS: ainsi, l'Office fédéral de l'informatique et de la télécommunication exploite différents systèmes d'information contenant des données en provenance de BV Plus et qui disposent, depuis cette année, d'une base légale suffisante. De plus, nous avons accompagné un projet de l'OFPER qui doit, en cas de transfert d'un collaborateur d'une unité à une autre au sein de l'administration, assurer que seules les données nécessaires à la nouvelle unité administrative ne lui soient communiquées. Jusqu'à présent, toutefois, aucune solution technique n'a pu être trouvée à ce problème. Nous suivrons de près l'évolution de la situation.

1.8 Économie et commerce

1.8.1 Stratégie énergétique 2050 et les compteurs intelligents

Nous nous sommes prononcés sur la stratégie énergétique 2050 dans le cadre de la procédure de consultation. Nos critiques ont porté sur l'absence de précision de la base légale concernant le traitement des données personnelles et nous avons demandé une modification à ce sujet. Nous avons également fourni suivi et conseils au groupe de travail Smart Grids Road Map Suisse.

De notre point de vue, les dispositions régissant les traitements de données personnelles figurant dans le projet soumis à consultation concernant la stratégie énergétique 2050 ne répondent pas aux critères de précision d'une base légale. Nous avons demandé que le but du système soit décrit de manière à être exactement reconnaissable par les personnes concernées. Plus les atteintes à la personnalité peuvent être graves (donc dans le cas de données sensibles et de profils de la personnalité), plus le degré de détail doit être élevé. Indépendamment de la nature des données personnelles traitées, il ne suffit pas de dire que la finalité du système est de permettre à l'organe fédéral responsable d'accomplir ses tâches légales. Au contraire, il faut donner une liste exhaustive des tâches pour lesquelles un traitement des données est prévu.

En ce qui concerne les compteurs intelligents et la protection des données, nous avons fourni suivi et conseils au groupe de travail de l'Office fédéral de l'énergie «Smart Grids Road Map Suisse». Nous sommes intervenus lors de plusieurs séances (cf. nos explications à ce sujet sur notre site www.leprepose.ch, Protection des données – Habiter et transports. La proportionnalité du traitement des données est un aspect essentiel dans le cas de la mise en place de ce type de compteur. En d'autres termes, seules les données nécessaires à la réalisation du but poursuivi doivent être traitées et les données qui ne sont plus nécessaires doivent être effacées, anonymisées ou agrégées.

1.8.2 Les cartes clients dans le commerce de détail

Cette année, le PFPDT a effectué des contrôles dans le domaine des cartes clients auprès des deux plus importants distributeurs de Suisse. L'analyse est encore en cours.

Plusieurs années se sont déjà écoulées depuis l'établissement des faits approfondi que nous avions effectué concernant les cartes clients auprès des deux grands distributeurs Migros et Coop (www.leprepose.ch, Protection des données –

commerce et économie – Données-clients). Dans le cadre de nos suivis, nous avons procédé cette année à un nouveau contrôle des traitements de données dans ce domaine. Nous avons saisi cette occasion pour examiner toutes les nouvelles offres et nouveaux services liés à ces cartes clients.

Ces contrôles nous ont permis de vérifier si les propositions d'amélioration issues des derniers examens ont bien été mises en œuvre et de soumettre les nouveaux traitements à un examen détaillé afin d'en vérifier la conformité avec les dispositions de protection des données. L'analyse des résultats de ces vérifications est encore en cours. Lors de nos inspections, nous avons heureusement pu constater que les deux grands distributeurs s'abstiennent toujours de commercialiser les données de leurs clients et qu'ils n'ont pas l'intention de le faire à l'avenir.

1.8.3 Utilisation commerciale de systèmes de localisation de personnes

On constate un usage croissant des systèmes de localisation de personnes pour analyser le comportement des clients et optimiser ainsi les espaces de vente, les gammes de produits et les offres de services. C'est pourquoi nous avons étudié quelques-uns de ces systèmes et pu constater qu'ils présentaient certains risques pour les droits de la personnalité.

Quiconque connaît le comportement de ses clients peut en tirer des avantages financiers, car cela lui permet d'optimiser les emplacements des espaces publicitaires, d'adapter la gamme de produits offerts ou même d'envoyer de la publicité personnalisée. De plus en plus d'entreprises veulent profiter de ces avantages et mettent en œuvre à cette fin des systèmes qui observent de manière entièrement automatisée les clients et analysent leur comportement. Les systèmes que nous avons étudiés détectent les personnes qui entrent dans un local donné (un centre commercial, par exemple) et suivent ensuite leurs déplacements à l'intérieur du local.

Certains systèmes misent sur des données biométriques (reconnaissance faciale), traitant ainsi incontestablement des données personnelles. Ils permettent en règle générale également de classer les personnes enregistrées, par exemple selon leur âge, sexe ou origine ethnique. Les risques d'une violation de la personnalité sont évidents, raison pour laquelle une attention particulière doit être accordée à la protection des données (cf. notre «Guide relatif aux systèmes de reconnaissance biométrique», sur notre site www.leprepose.ch, dans la rubrique Protection des données – Biométrie).

D'autres systèmes utilisent par contre les signaux émis par les téléphones mobiles et enregistrent le déplacement de tout appareil qui se trouve à l'intérieur du

local surveillé. Même si cette méthode ne semble, à première vue, pas collecter de données personnelles (les opérateurs de ces systèmes ne pouvant pas, par exemple, identifier une personne sur la base du numéro TMSI ou IMSI d'un téléphone mobile), il est relativement facile, dans certains cas, d'établir une relation avec une personne donnée d'une manière indirecte: le profil de déplacement qui en résulte peut éventuellement permettre d'attribuer le profil initialement non personnel à une personne donnée.

Ainsi, par exemple, les profils de déplacement du personnel d'un magasin sont en règle générale très différents de ceux de la clientèle. S'il s'agit en plus d'une petite équipe, il est relativement facile d'attribuer un profil à un collaborateur précis. Par ailleurs, la mise en relation avec d'autres données (tels que des enregistrements des caméras de surveillance) peut également permettre de personnaliser des profils qui à l'origine étaient impersonnels. On peut donc admettre que ces systèmes traitent des données personnelles et qu'ils doivent donc respecter les principes de traitement de la loi sur la protection des données.

Cela signifie en premier lieu que le traitement de données doit être légitimé par un motif justificatif. Dans le cadre de l'exploitation de tels systèmes, ce motif pourrait être un intérêt prépondérant ou le consentement des personnes concernées:

- Un intérêt prépondérant est présumé dans les cas où de tels systèmes sont, par exemple, utilisés pour améliorer la sécurité des bâtiments d'un aéroport ou d'une gare. Un intérêt prépondérant existe également lorsque les systèmes sont utilisés à des fins ne se rapportant pas à des personnes, par exemple pour une analyse purement statistique du trafic client dans laquelle les personnes ne sont pas identifiables.
- En revanche, les analyses personnelles à des fins de marketing ne peuvent pas être justifiées par un intérêt prépondérant. Le traitement des données doit donc être justifié par le consentement des personnes concernées. Il y a lieu de tenir compte du fait que le consentement doit toujours être donné de plein gré, que les personnes concernées doivent donc avoir la possibilité de se déplacer à l'intérieur d'un bâtiment surveillé par un système de localisation sans être détecté par le système. L'application concrète de cette exigence peut, en fonction de la configuration du système, s'avérer très difficile.

La surveillance du comportement des employés par le biais de systèmes de localisation est absolument exclue. Une telle utilisation ne peut pas être justifiée, pas même avec le consentement des employés concernés, et est donc illégale.

Pour plus d'informations à ce sujet, consulter notre site www.leprepose.ch, sous la rubrique Protection des données – technologies.

1.8.4 Droit à l'oubli au registre du commerce

Le projet de loi sur la modernisation du registre du commerce ne prévoit pas d'introduire un «droit à l'oubli». Au vu des résultats de la procédure de consultation, l'Office fédéral du registre du commerce conclut que la publication de données sur Internet ne nécessiterait pas de règles particulières. Nous regrettons cette décision.

Dans notre 20e rapport d'activités 2012/2013, ch. 1.8.4, nous nous étions exprimés sur les propositions de modification du registre du commerce. Nous y avions notamment salué le fait que l'Office fédéral du registre du commerce (OFRC) avait adopté dans le projet mis en consultation un droit à l'oubli adapté au registre du commerce. La consultation a pris fin au cours de l'année passée sous revue.

Se fondant sur les résultats de la consultation, l'OFRC n'entend désormais pas examiner plus en détail la possibilité d'interdire la libre consultation des données du registre du commerce sur Internet. Cinq participants de la consultation auraient en effet été d'avis que la publication sur Internet ne devrait pas être soumise à des règles particulières. Nous ne pouvons pas nous rallier à cette argumentation. À notre sens, il y a lieu de distinguer entre la tenue physique des données dans les registres du commerce et la manière dont ce contenu est publié.

Lors de différentes séances et prises de position, nous avions attiré l'attention de l'OFRC sur la problématique d'une publication de données du registre du commerce indéfiniment accessibles sur Internet. La problématique s'est encore aggravée depuis que certains registres du commerce se sont mis aussi à publier rétroactivement les pièces justificatives telles quelles sur Internet. À titre d'exemple, les adresses privées de conseillers d'administration, les extraits de procès-verbaux pouvant contenir des données personnelles sensibles, des numéros de passeports et de cartes d'identité, etc. sont désormais accessibles à un large public. Nous déplorons vivement la démarche de l'OFRC, d'autant plus que la problématique décrite est encore renforcée par les pratiques des sociétés de renseignements privées. Nous avons également décrit la problématique de la publication de données d'état civil sur Internet dans le présent rapport d'activités, ch. 1.2.10.

De plus, il est prévu d'introduire le numéro d'assuré AVS comme identificateur dans le registre du commerce. Même si elle ne sera accessible qu'en interne par l'administration, cette nouvelle extension de l'application du numéro d'assuré est problématique du point de vue de la protection des données (voir chiffre 1.5.3 du présent rapport d'activités).

1.8.5 Enquêtes dans le domaine des agences de renseignement économique et de renseignement en matière de crédit

Le suivi de la mise en œuvre de notre recommandation dans l'affaire «Moneyhouse» a pris un certain temps. Depuis que la société qui exploite ce service, itonex AG, a modifié ses procédures de suppression des données, de nombreuses personnes s'en plaignent. Nous les conseillons et sommes en train d'examiner les prestations proposées par itonex AG.

Dans notre 20e rapport d'activités 2012/2013, au ch. 1.8.2, nous avons rendu compte de notre dernier examen des faits, qui avait pour objet notamment la publication d'adresses sur Internet. La société itonex AG, qui exploite le portail concerné, avait accepté nos recommandations.

La conclusion de cette première partie de notre examen des faits ainsi que les mesures d'accompagnement de l'application de la recommandation a nécessité plus de temps que prévu. La modification des modalités de suppression des données par la société a eu pour conséquence que de nombreuses personnes se sont adressées à nous parce qu'elles s'opposaient à devoir fournir à l'entreprise la copie d'une pièce d'identité officielle. La principale critique exprimée à ce sujet était que l'on voulait éviter de fournir encore plus d'informations à une entreprise qui publiait des données sur Internet sans autorisation préalable.

Conformément aux dispositions de la loi sur la protection des données, une entreprise doit procéder à une authentification, c'est-à-dire vérifier si la personne qui veut faire valoir son droit de suppression est bel et bien la personne concernée. Elle peut à cet effet utiliser diverses méthodes, qui doivent être adaptées aux exigences en matière de protection des données. Nous avons conseillé aux personnes concernées de constater en premier lieu quelles sont les données personnelles qu'itonex AG possède déjà, puis de noircir toutes les autres informations sur la copie de la pièce d'identité. Ces recommandations sont également disponibles sur notre site www.leprepose.ch, Protection des données – commerce et économie – crédit et encaissement.

Nous continuons à recevoir des plaintes de personnes qui sont inscrites au registre du commerce et dont les données sont également publiées sur le site www.moneyhouse.ch. À ce sujet, nous nous permettons de rappeler qu'il existe un jugement exécutoire du Tribunal administratif fédéral (cf. www.leprepose.ch, Protection des données – commerce et économie – registre du commerce). Tant qu'itonex AG affiche les informations contenues dans le registre du commerce gratuitement et de manière complète, ces informations ne peuvent pas être supprimées (chiffre 1.8.4 du présent rapport d'activités).

Dans une deuxième phase de notre examen des faits, nous sommes actuellement en train d'analyser les autres prestations de services offertes par la société itonex AG. Vu l'envergure des traitements de données qu'elle effectue, cette analyse va encore prendre un certain temps.

1.8.6 Suppression d'adresses dans les banques de données sur la solvabilité

Les administrateurs de banques de données sur la solvabilité doivent prendre en compte les besoins de sécurité allégués lors de demandes de suppression.

Nous recevons régulièrement des demandes de personnes qui désirent faire supprimer leur adresse d'un fichier sur la solvabilité. Selon la loi sur la protection des données, une agence de renseignement est autorisée, pour l'examen de la solvabilité, à traiter des données contre la volonté de la personne concernée, pour autant qu'elle ne traite pas des données sensibles ou des profils de la personnalité. Au cas où une personne fait valoir des motifs de sécurité pour la suppression de ses données, ces arguments doivent être pris en compte dans la pesée des intérêts effectuée au cas par cas. À notre avis, l'adresse devrait être supprimée.

La personne concernée doit toutefois être consciente que le fait qu'elle soit introuvable dans les banques de données sur la solvabilité peut présenter des inconvénients pour ses relations d'affaires. Ainsi, ceci peut rendre difficile ou impossible l'obtention d'un crédit par le biais d'Internet. Les agences de renseignement sont autorisées à communiquer le fait qu'une personne n'apparaît pas dans une banque de données sur la solvabilité, mais ne peuvent pas en conclure que cette personne n'est pas solvable.

1.8.7 Échange de données concernant des vols dans les commerces

Une enseigne et ses magasins affiliés peuvent, à certaines conditions, collecter des informations concernant des personnes appréhendées pour vol, notamment afin d'évaluer l'opportunité de porter plainte. L'échange systématique des cas de vol entre les différentes enseignes dans le cadre d'une banque de données centralisée est cependant contraire au principe de proportionnalité.

Une société de sécurité privée a sollicité notre avis concernant la mise en place d'une banque de données centralisée recueillant systématiquement les cas de vol enregistrés dans les commerces de détail. L'échange, entre les enseignes

commerciales, des informations concernant des personnes appréhendées pour vol devait permettre en premier lieu d'apprécier l'opportunité de porter plainte et d'adapter les sanctions ou les mesures en cas de récidive. Le concept présenté prévoyait également que les autorités de police ou de poursuite pénale puissent elles-mêmes accéder au fichier par procédure d'appel, afin de détecter plus aisément les cas de récidive, de vol par métier ou en bande organisée.

S'agissant des traitements de données effectués par les enseignes commerciales, ceux-ci doivent, conformément à la LPD, respecter les principes généraux de la protection des données et se fonder sur un motif justificatif. En l'absence de consentement et de base légale spécifique permettant la saisie et l'échange de ces données par le biais d'une plateforme commune, nous avons examiné si les enseignes commerciales pouvaient se prévaloir d'un intérêt privé ou public prépondérant.

La société de sécurité a d'abord invoqué l'intérêt public de la lutte contre le vol. Cette dernière est cependant avant tout une tâche publique qui relève des autorités de police et de justice compétentes et qui nécessite une base légale. Des enseignes commerciales ou une société de surveillance privée ne peuvent en l'occurrence se fonder sur un intérêt public prépondérant pour se substituer, sans mandat, aux autorités dans l'exécution de tâches typiquement policières et communiquer, de façon systématique, des données sensibles à d'autres personnes privées, alors même qu'il est question ici de délits mineurs contre le patrimoine, et non d'infractions présentant un danger pour la vie ou l'intégrité corporelle. L'enseigne commerciale ou le magasin concerné a par ailleurs toujours la possibilité de communiquer les données à la police dans le cadre d'une plainte ou d'une dénonciation pénale. De leur côté, les autorités de poursuite pénale ont, dans le cadre d'une procédure, la possibilité d'exiger les données contenues dans un fichier.

Nous avons ensuite examiné si les enseignes commerciales pouvaient se fonder sur un intérêt privé prépondérant. Il convient à cet égard de distinguer entre le traitement des données personnelles dans le cadre du fichier interne de l'enseigne commerciale et la communication des données à d'autres enseignes commerciales dans le cadre d'un fichier commun.

Un intérêt privé prépondérant peut généralement être admis pour le traitement de données dans le cadre d'un fichier interne, pour autant que les principes généraux de la protection des données soient respectés. L'enseigne commerciale peut enregistrer les cas de vol survenus dans ses magasins affiliés afin de préserver la possibilité de déposer plainte auprès de la police ou de mettre en œuvre une autre mesure telle qu'une interdiction de magasin ou d'enseigne. Les magasins affiliés à une même enseigne peuvent donc, indépendamment de leur localisation en Suisse, échanger leurs données; sur cette base, l'enseigne commerciale pourra évaluer la

situation et adapter les mesures, comme par exemple décider de l'opportunité ou non de porter plainte. Dans le cadre d'une plainte ou d'une dénonciation pénale, l'enseigne commerciale ou le magasin concerné pourra alors communiquer ces données à la police.

Après une pesée des intérêts en présence, nous sommes arrivés à la conclusion qu'au-delà de la gestion des cas de vol dans le cadre d'un fichier interne, l'échange systématique et automatisé des données entre les différentes enseignes commerciales n'est pas conforme au principe de proportionnalité. Il existe en effet d'autres moyens moins attentatoires à la sphère privée: le fait que pour des raisons d'opportunité, les enseignes commerciales ne souhaitent pas, dans les cas envisagés, porter plainte à chaque fois, est compréhensible. Toutefois, si elles ne font pas valoir les moyens de droit existants, elles ne pourront faire valoir ensuite un intérêt privé prépondérant pour transmettre, en plus de façon systématique, des données sensibles aux autres commerces et créer ainsi un casier judiciaire privé parallèle spécifique aux cas de vols dans (tous) les commerces de détail. De plus, il convient de relever qu'il est question ici de délits mineurs contre le patrimoine, et non d'infractions présentant un danger pour la vie ou l'intégrité corporelle.

1.8.8 Outil d'analyse d'impact relative à la protection des données

Dans le cadre de nos activités de sensibilisation à la protection des données et suivant la tendance actuelle du «Privacy by design», nous avons développé un outil d'analyse d'impact relative à la protection des données. Cet outil offre un questionnaire qui évolue de manière dynamique en fonction des réponses déjà apportées. À la fin de l'exercice, une évaluation personnalisée permet aux participants de se positionner par rapport à leur approche de la protection des données dans le projet qu'ils ont choisi d'évaluer.

Le concept du «Privacy by design» s'inscrit dans le courant actuel de l'anticipation des problèmes de protection des données lors de la conception et du développement de nouveaux produits. Dans ce contexte, nous avons développé un outil d'analyse d'impact relative à la protection des données. Le but de cet outil est de permettre aux acteurs impliqués dans la conception puis dans la réalisation de nouveaux produits ou de nouvelles applications de procéder à une première évaluation et de détecter de manière anticipée les problèmes de protection des données auxquels ils vont être confrontés afin de prendre rapidement les mesures adéquates.

L'outil se présente sous la forme d'un questionnaire dynamique: les questions sont affichées tour à tour en fonction des réponses apportées précédemment. Le questionnaire s'adapte donc ainsi à chaque utilisateur: les grands axes du

questionnaire sont définis par la provenance de l'utilisateur qui représente le secteur privé ou un organe fédéral et par les catégories de données personnelles utilisées, en particulier les données sensibles. Le questionnaire se subdivise en plusieurs chapitres qui traitent par exemple de la collecte, de la transmission et de la sauvegarde des données mais également des mesures techniques et organisationnelles à mettre en place.

Une fois le questionnaire rempli, une évaluation adaptée est produite et présentée à l'utilisateur. Cette évaluation se compose d'un score calculé en fonction des réponses apportées ainsi que d'une liste de commentaires. Pour chaque section de l'évaluation, un commentaire générique explique différents aspect de la protection des données. De plus, si durant le questionnaire l'utilisateur a répondu de manière telle qu'il peut être déduit qu'un aspect en particulier n'est pas pris en compte ou mal considéré, un commentaire spécifique lui indique les potentiels manquements en matière de protection des données dans la conception de son projet.

Cet outil de sensibilisation se veut simple et détaché des bases légales en vigueur afin d'être accessible au plus grand nombre. Il a été conçu de manière à respecter la protection des données, c'est-à-dire en ne conservant aucune donnée des utilisateurs. Il est accessible depuis notre site www.leprepose.ch, sous la rubrique «Liens».

1.8.9 Projet de système d'accueil hôtelier

Nous avons reçu une demande d'avis concernant la mise en place d'un système d'accueil destiné au marché hôtelier de luxe, collectant les mouvements et les préférences des clients à l'aide de la technologie RFID. Un tel profilage nécessite une information préalable des personnes concernées ainsi que leur consentement explicite. Une alternative doit être proposée. La collecte des données et tout traitement ultérieur, notamment l'évaluation des données, doivent en particulier être reconnaissables pour les personnes concernées.

Une start-up nous a consultés concernant la mise en place d'un système d'accueil destiné au marché hôtelier de luxe, impliquant la collecte des mouvements et des préférences des clients à l'aide de la technologie RFID. Conformément au projet, chaque client reçoit un petit porte-clefs doté d'une puce RFID, en remplacement ou en complément d'une carte d'accès classique. La technologie RFID permet, grâce à l'installation d'antennes, de localiser le client dans l'hôtel en temps réel.

En plus des données d'identification, les souhaits et préférences des clients sont collectés, tels que les horaires de nettoyage, la température ou l'éclairage de la chambre, les espaces de l'hôtel fréquentés ou encore les plats appréciés.

Ce système doit permettre de personnaliser l'accueil des clients en leur offrant des services individualisés, et d'optimiser la gestion du personnel en fonction notamment de l'affluence des clients aux différents espaces de l'hôtel.

Une telle collecte de données étant soumise à la loi fédérale sur la protection des données (LPD), nous avons donné notre appréciation quant à l'utilisation d'un tel système: les traitements envisagés doivent être justifiés par un motif justificatif. En l'absence de base légale ou d'intérêt prépondérant, seul le consentement des personnes concernées peut, à certaines conditions, justifier le traitement des données des clients dans le cadre du système d'accueil hôtelier. Pour que le consentement soit valable, il doit être libre et éclairé: la participation doit être facultative (volontaire) et une alternative doit être proposée.

Le client doit toujours avoir la maîtrise sur ses données et un consentement peut être révoqué en tout temps. Le client devra être informé au préalable des traitements de données effectués ainsi que de leurs finalités. Les données collectées pouvant constituer un profil de personnalité, le consentement doit être explicite: ce dernier pourra être requis sous forme de signature au moment de la remise de la puce RFID après une explication concernant la collecte des données effectuée.

En outre, il convient de veiller à ce que les principes fondamentaux de protection des données soient respectés, d'autant plus que les données collectées peuvent en l'occurrence constituer un profil de personnalité (protection accrue). En particulier, toute collecte de données et tout traitement ultérieur, tel que l'évaluation des données, doivent être reconnaissables pour les personnes concernées.

En application du principe de proportionnalité, les données traitées doivent être limitées à celles qui permettent d'atteindre l'objectif visé et qui présentent un rapport raisonnable entre l'atteinte à la personnalité et la finalité du traitement. Dans le cas particulier, il paraîtrait en particulier disproportionné de tracer les clients précisément dans tout l'établissement hôtelier; il conviendra de limiter les zones captées par les antennes. Une indication de présence à l'étage ou au moment d'entrer dans un espace donné (p.ex. réception, restaurant, spa) ou d'en sortir paraît suffire eu égard aux buts poursuivis.

De plus, seules les personnes ayant effectivement besoin des données considérées doivent pouvoir y accéder à un moment donné; par exemple, le personnel de nettoyage a uniquement besoin de savoir si (ou quand) une chambre peut être nettoyée, et non où la personne se trouve précisément. L'exigence de proportionnalité limite également le traitement de données sur l'échelle temporelle. Dès que les données personnelles ne sont plus utiles pour le but poursuivi, elles doivent être détruites ou rendues anonymes.

Selon le principe de finalité, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte ou qui ressort des circonstances. À moins que le client y ait expressément consenti, les données ne pourront par exemple être transmises à des tiers à des fins de marketing.

Selon le principe de sécurité, les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Le choix du Cloud computing n'est en l'occurrence pas approprié pour le traitement de profils de personnalité. De plus, il faut être conscient que les données privées des clients fréquentant les hôtels de luxe pourraient, encore plus que d'autres, être la cible de hackers et que le risque que des personnes mal intentionnées cherchent à accéder indûment aux données personnelles de personnalités connues ou fortunées est plus important. Dans la mesure où des données devaient également être transmises à l'étranger, il conviendra au préalable de vérifier qu'elles seront soumises à une législation assurant un niveau de protection adéquat. Faute de législation équivalente, les données personnelles ne peuvent être communiquées qu'à certaines conditions déterminées.

Outre le respect des principes et des devoirs mentionnés, le maître du fichier doit notamment veiller à la mise en œuvre du droit d'accès. Il est également tenu de déclarer le fichier au préposé pour enregistrement.

Nous sommes arrivés à la conclusion que l'utilisation de ce système d'accueil hôtelier était délicat du point de vue de la protection des données. Les clients des hôtels mettant en place le système doivent avoir le choix d'y participer ou non. Vu la constitution éventuelle de profils de personnalité, les traitement de données nécessitent dans tous les cas une information adéquate et le consentement explicite des personnes concernées. Une alternative pour les personnes refusant l'utilisation de la technologie RFID doit être proposée.

1.8.10 Révision de la loi fédérale et de l'ordonnance sur les produits de construction

La consultation des offices sur les produits de construction qui a commencé au printemps de 2012 a soulevé quelques questions concernant le principe de la légalité, notamment quant aux exigences concernant la densité normative lors du traitement de données sensibles par des organes fédéraux.

Sous la conduite du Département fédéral des finances (DFF), respectivement de l'Office fédéral des constructions et de la logistique (OFCL), la consultation des offices sur la révision de la loi et de l'ordonnance sur les produits de construction a été lancée au printemps 2012. Afin d'éviter que la Suisse soit défavorisée sur

le plan économique, la Confédération s'efforce constamment d'harmoniser ses prescriptions techniques avec le droit international. L'objectif du projet est d'éliminer des différences majeures entre le nouveau droit européen et le droit suisse sur les produits de construction.

À cette fin, deux mesures ont été prises: d'une part, on a développé un nouveau concept pour la commercialisation de produits de la construction, d'autre part il est prévu d'adapter la surveillance du marché. Afin de répondre aux nouvelles exigences en matière de surveillance du marché, il est nécessaire de mettre en place au niveau fédéral une banque de données relative à l'exécution. Le projet de loi prévoit que des données sensibles y sont aussi traitées, telles que les sanctions administratives ou poursuites pénales relatives à l'activité des fabricants de produits de construction. Il faudra donc tenir compte des exigences plus strictes lors de l'élaboration de la base légale, notamment au niveau de la densité normative.

Dans nos prises de position, nous avons fait part essentiellement de quatre remarques à ce sujet:

- Premièrement, la désignation de la finalité du traitement des données est à notre avis trop générique. La finalité de la banque de données étant de surveiller le marché, ceci doit clairement ressortir du texte de la loi.
- Deuxièmement, nous nous sommes exprimés sur l'introduction d'un renvoi dans le texte de la loi aux dispositions administratives et pénales.
- Troisièmement, nous avons insisté pour que l'on désigne un maître de fichier et avons proposé que ce soit l'OFCL.
- Notre dernière remarque concerne la liste des organisations professionnelles qui peuvent également être chargées de tâches de surveillance du marché; celles-ci ne sont mentionnées nulle part de manière explicite dans le projet; il n'en est fait mention que sous le terme générique d'organes de surveillance du marché.

De ces quatre principales demandes, les trois premières ont été prises en compte et appliquées dans le projet de loi. Le dernier point concernant la désignation des autorités de surveillance du marché impliquées dans le traitement de données sensibles, entre autres, n'a pas été pris en considération. Nous avons toujours souligné dans nos prises de position que les divergences ne pouvant être prises en compte devaient être mentionnées dans la proposition au Conseil fédéral.

1.9 Finances

1.9.1 Constatation des faits auprès d'un prestataire de services financiers

Nous avons ouvert une procédure d'établissement des faits à l'encontre d'un prestataire financier en été 2012, afin de clarifier si la collecte et la gestion des informations respectaient les exigences de la protection des données.

La première étape de la procédure, consistant à constater les faits en collaboration avec la banque, est close (cf. notre 20e rapport d'activités 2012/2013, ch. 1.8.7). Cette phase, lors de laquelle l'entreprise contrôlée n'a pas seulement une obligation de coopérer mais également la possibilité de prendre position, constitue l'assise du rapport final dans lequel les considérants en droit seront traités.

À l'heure actuelle, la procédure suit son cours.

1.9.2 Éclaircissements concernant les cartes bancaires sans contact

Nous avons dressé un état des lieux sur la fonction de paiement sans contact des cartes de crédit, suite à une collaboration sommaire avec la CNIL et une prise de contact avec les principales émettrices de cartes bancaires.

Depuis l'année dernière, les médias se sont saisis du thème des cartes de crédit permettant un paiement sans contact. Différents types d'analyses et de conclusions y sont développées, pour la plupart préoccupantes en termes de droits de la personnalité et de sécurité des données. Quelques-unes de ces thèses ont été corroborées par la Commission nationale de l'informatique et des libertés (CNIL) dans sa communication du 1er juillet 2013 «Sécurité des cartes bancaires sans contact: quelles sont les avancées et les améliorations possibles?». Nous avons, sur cette base-là et dans le cadre de nos attributions légales, entamé un bref échange de renseignements avec l'autorité française. Ce qui nous a permis dans un premier temps d'évaluer les informations qui circulent tant sur la toile que dans la presse écrite. Dans la foulée, un contact a également été établi avec les principales émettrices de cartes de crédit en Suisse afin de leur donner l'occasion de prendre position.

Les nouvelles cartes mises en circulation en Suisse dès l'année dernière sont, pour la plupart, d'ores et déjà dotées d'une technologie de radio-identification (RFID), qui permet un paiement sans contact dans différents points de ventes équipés de terminaux compatibles (Point of Sale, POS). Les trois grands donneurs de licence de

cartes de crédit MasterCard, Visa et American Express ont mis sur pied un produit similaire portant toutefois des noms différents. Il s'agit des systèmes PayPass, payWave et ExpressPay. Ces dénominations – qui d'ailleurs figurent généralement sur la carte – donnent déjà une petite idée sur le mode de fonctionnement: en passant la carte à proximité d'un POS, le paiement est comptabilisé sans devoir introduire de code ou apposer une signature sur la facture. L'identification s'opère, dans ce cas, par fréquences radio. Les données nécessaires à l'achat sont transmises par ce biais depuis la carte au terminal. Un processus d'authentification, par exemple au moyen d'un numéro d'identification personnel (NIP) n'intervient en principe pas. L'opération est néanmoins limitée à un montant maximum afin de restreindre le dommage en cas de perte ou de vol.

La transmission de données décrite ci-dessus n'est pas réservée aux terminaux de ventes POS. Par conséquent, un résultat non désiré peut être l'interception et la lecture, à l'insu du titulaire de la carte, par un tiers non autorisé, équipé du minimum technologique nécessaire. Un risque accru existe notamment dans les lieux publics.

Suite à l'état des lieux sur le thème de la sécurité de l'information – étroitement lié à la responsabilité civile du maître du fichier (à savoir l'émetteur de cartes de crédit) – il convient d'aborder la question de l'autodétermination informationnelle. Ce droit, fondamental et inaliénable, ancré dans la Constitution fédérale, prévoit que toute personne peut s'opposer à un traitement. Ce droit peut subir des restrictions, comme tout droit fondamental, mais seulement à des conditions précises. En l'occurrence, la LPD prévoit des motifs justificatifs permettant un traitement en toute licéité: le consentement, l'intérêt privé ou public prépondérant ou la loi. Or, en l'espèce, les émettrices consultées ne font valoir aucun intérêt prépondérant privé ou public au traitement décrit. L'insertion de la puce RFID dans la carte n'est de surcroît pas soumise au choix ou au consentement du client. Il est vrai que la politique d'information des émettrices consultées correspond aux préceptes de la transparence, mais elle ne suffit pas à inférer un consentement de la part du client.

Admettons qu'un consentement tacite au traitement suffise, puisqu'a priori aucune donnée sensible n'est communiquée depuis la puce. Dans ce cas, les éléments constitutifs du consentement doivent également être remplis. Il s'agit d'une part de l'aspect «éclairé» et d'autre part du caractère «libre» relatif à la formation de la volonté du concerné. Ici, le noyau du problème se situe au niveau du consentement libre. Dans les faits, la situation actuelle sur le marché suisse des cartes de crédit sans contact favorise un déséquilibre structurel entre le client et la banque. En effet, une alternative, à savoir le choix d'un concurrent offrant un produit de même gamme, substituable, sans RFID, n'existe a priori pas. Un consentement tacite par le biais des conditions générales ne remplit dès lors pas les critères intangibles du consentement libre.

Nous appelons le secteur bancaire à une adaptation des mesures pour le respect des libertés individuelles, notamment en octroyant un choix aux clients ou la possibilité d'un refus de la technologie. En attendant cette évolution, nous rendons les porteurs de cartes de crédit qui souhaitent protéger leurs données attentifs à la possibilité de les mettre dans des portemonnaies conçus pour bloquer la transmission des fréquences radios ou dans des fourres en aluminium.

1.9.3 Communication de données à des autorités fiscales étrangères

Différents projets de lois avaient pour objet la communication de données à des autorités fiscales étrangères. Dans le cadre des travaux législatifs, nous avons fait part de nos positions concernant le Foreign Account Tax Compliance Act FATCA et la loi sur l'assistance administrative en matière fiscale.

Au cours de l'année sous revue, nous avons pris position sur différents projets de lois réglementant la transmission de données fiscales à des autorités étrangères. Nous nous exprimons comme suit sur le Foreign Account Tax Compliance Act (FATCA) et sur la loi sur l'assistance administrative en matière fiscale:

Foreign Account Tax Compliance Act (FATCA)

Dans notre 19e rapport d'activités 2011/2012, ch. 1.9.1, nous avons rendu compte de cette loi fiscale américaine et des traitements de données qu'elle implique, à notre avis problématiques. L'accord a été signé par la Suisse le 14 février 2013 et a en même temps été mis en consultation, accompagné d'une loi d'application. Fondamentalement, il existe deux modèles de cet accord, la Suisse ayant décidé de reprendre le modèle 2. Les modèles constituent tous deux une forme d'échange automatisé d'informations.

À la différence du modèle 1, le modèle 2 implique que les FFI (Foreign Financial Institutes, soit les banques, assurances, etc.) rendent compte directement à l'autorité fiscale américaine (Internal Revenue Service, IRS). Selon le Secrétariat d'État aux questions financières internationales (SFI), le secret fiscal serait ainsi mieux préservé. Les titulaires américains d'un compte qui ne fournissent pas de consentement à la communication de ces données peuvent défendre leurs intérêts avant la communication de ces données à l'IRS. Actuellement, des tendances législatives visent toutefois à restreindre ces droits.

Nous avons été invités à une séance de la Commission de l'économie et des redevances (CER) du Conseil national, et avons saisi cette opportunité pour exprimer nos doutes. Nous avons notamment déploré que de nombreuses incertitudes

subsistaient encore au moment de la discussion parlementaire des projets de lois. Il n'était ainsi pas précisé comment s'organiseraient les contrats entre les FFI et l'IRS, ni quels principes de traitement y seraient pris en compte (notamment la possibilité de rectification et le principe de traitement proportionné des données). Le Parlement a approuvé l'accord et le projet de loi. Entre-temps, l'IRS a reporté l'introduction de FATCA à juillet 2014.

Loi sur l'assistance administrative fiscale

La loi sur l'assistance administrative fiscale est entrée en vigueur le 1er janvier 2013. En raison de différents développements internationaux, il a fallu l'adapter au cours de l'année. Nous n'avons malheureusement pas été invités à prendre position lors de la consultation ordinaire des offices, raison pour laquelle nous avons rédigé un rapport à l'intention du Conseil fédéral, qui devait adopter le message relatif à la révision de la loi sur l'assistance administrative fiscale. Nous y avons critiqué la procédure d'information ultérieure de la personne habilitée à recourir. Celle-ci avait jusqu'alors la possibilité de se défendre par voie de droit contre la transmission d'informations fiscales à une autorité requérante à l'étranger, avant qu'elle n'ait lieu.

Désormais, la personne habilitée à recourir pourrait n'être informée qu'après transmission des informations par l'Administration fédérale des contributions (AFC), si l'autorité requérante (à l'étranger) rend vraisemblable que la communication préalable pourrait mettre en danger le but de l'entraide judiciaire ou le succès de l'enquête. Nous avons critiqué la formulation insuffisamment définie des dérogations et le manque de transparence des traitements de données. La transparence en tant que principe de protection des données est indispensable pour qu'une personne puisse exercer ses droits en matière de protection de la personnalité. Le Conseil fédéral a refusé notre proposition. Le thème de la transmission de données fiscales à des autorités étrangères est aussi traité au chiffre 1.9.5 du présent rapport d'activités.

1.9.4 Recommandations révisées du Groupe d'action financière (GAFI)

Le Secrétariat d'État aux questions financières internationales SFI a mis en consultation auprès des offices différentes modifications de lois destinées à mettre en œuvre les recommandations du GAFI au niveau national. Nous avons pris position sur divers points.

Dans le cadre des travaux législatifs pour la mise en œuvre des recommandations du GAFI, nous nous sommes exprimés sur l'introduction d'obligations de déclarer pour les titulaires d'actions au porteur, sur la définition des personnes politiquement exposées au niveau national, sur les listes terroristes et sur la création d'une

structure interdépartementale pour la lutte contre le blanchiment d'argent, sur l'évaluation des risques et sur la manière d'assurer la cohérence de la politique suisse avec l'évolution internationale. Les modifications de lois prévues doivent permettre d'obtenir les résultats suivants:

- Une amélioration de la transparence pour les personnes morales, avec notamment l'introduction d'obligations de déclarer pour les titulaires d'actions au porteur.
- L'extension de la notion de personnes politiquement exposées aux personnes nationales et aux ressortissants d'organisations intergouvernementales, et l'introduction de devoirs de diligence appropriés pour les intermédiaires financiers.
- Les délits fiscaux graves seront considérés comme des infractions préalables au blanchiment d'argent.
- Les paiements en espèces supérieurs à CHF100 000 devront passer par un intermédiaire financier soumis à la législation sur le blanchiment d'argent.
- Une amélioration du système d'annonce de soupçons, allégeant ainsi le travail du Bureau de communication en matière de blanchiment d'argent (MROS).
- Une mise en œuvre améliorée de la recommandation GAFI relative aux sanctions ciblées en matière de financement du terrorisme. Il est prévu de créer un groupe de travail interdépartemental à cet effet.

On observe qu'un grand nombre d'articles de lois ont, en très peu de temps, dû être évalués sous l'aspect de la protection des données. Nous nous sommes donc concentrés sur quelques points, reportés ci-dessous. À notre avis, l'introduction d'obligations de déclarer pour les titulaires d'actions au porteur et les obligations de documentation correspondantes des entreprises entraînent un grand nombre de nouvelles banques de données. Le risque de violations des droits de la personnalité s'en trouve ainsi considérablement accru. Par ailleurs, le message relatif à la loi sur le blanchiment d'argent (LBA) cite effectivement quelles sont les personnes à définir comme proches de personnes politiquement exposées. Le cercle de ces personnes a cependant été défini de manière trop imprécise dans la loi, ce qui oblige les intermédiaires financiers à traiter des données personnelles d'un volume disproportionné.

Quant à la transmission de listes terroristes par le Département fédéral des finances aux intermédiaires financiers, nous avons relevé que les droits des personnes concernées, notamment le droit de rectification, doivent être garantis, et que l'exercice de ces droits est menacé par le manque de transparence du traitement

des données. En dernier lieu, nous nous sommes exprimés sur le manque de clarté des indications relatives à la création d'un groupe de travail interdépartemental. Le Secrétariat d'État aux questions financières internationales a pris acte de nos doutes sur le respect du principe de légalité et les a partiellement pris en compte.

1.9.5 Transmission de données de polices d'assurance à l'IRS

Une transmission de données à l'autorité fiscale américaine IRS peut, dans les cas où il s'agit de dépister un délit fiscal, contenir des données autres que simplement financières.

Le droit suisse connaît plusieurs moyens permettant de garantir un prêt bancaire par une assurance-vie, notamment la cession et le nantissement. Ces deux actes juridiques sont soumis à des exigences de forme strictes définies par la loi fédérale sur le contrat d'assurance (LCA). L'une de ces exigences est la remise de la police d'assurance au garant, dans ce cas la banque. Or, dans le cadre d'une procédure d'entraide administrative entre l'autorité fiscale américaine IRS et l'Administration fédérale des contributions (AFC), il est possible que l'on demande la remise de la police pour dépister un délit fiscal. La question se pose dans ce cas de savoir si la police peut être transmise et, dans l'affirmative, sous quelle forme. La question se pose également de savoir à qui l'on doit s'adresser si on est concerné par une telle procédure.

En tant qu'autorité fédérale de première instance, l'AFC est soumise à la loi fédérale sur la protection des données (LPD). Celle-ci est applicable aussi bien pour les procédures administratives de première instance que pour les procédures d'entraide administrative. La Convention entre la Confédération suisse et les États-Unis d'Amérique en vue d'éviter les doubles impositions en matière d'impôts sur le revenu (CDI CH-USA) est également applicable aux données d'assurance qui sont, par exemple, déposées auprès d'une banque suisse. Les dispositions des deux actes législatifs sont applicables en parallèle; dans les cas cependant où la CDI CH-USA contient des dispositions divergentes de la LPD, celle-ci prévaut alors en tant que loi spéciale.

Selon la LPD, un organe fédéral ne peut traiter des données personnelles que si une base légale suffisante existe à cet égard. La communication transfrontalière à une autorité étrangère est considérée comme un traitement de données et nécessite par conséquent une base légale. D'autres conditions doivent être respectées lors du traitement de données sensibles ou de profils de la personnalité: les organes fédéraux ne sont autorisés à traiter de telles données que si cela est prévu par une loi au sens formel, si la personne concernée a donné son consentement pour

ce cas particulier ou si elle a rendu ses données publiquement accessibles sans s'opposer explicitement au traitement.

La CDI CH-USA est considérée comme une loi au sens formel et peut donc justifier une communication de données par l'AFC à l'IRS, pour autant que les exigences concernant la communication stipulées à l'article 26 CDI CH-USA sont remplies.

Selon cette disposition, la divulgation, sous forme de copie certifiée conforme, d'une police d'assurance entreposée auprès d'une banque n'est autorisée que si cela est nécessaire pour l'exécution des dispositions de la CDI CH-USA ou pour la prévention de fraudes ou de délits semblables. De plus, une communication par l'IRS à d'autres autorités n'est autorisée que dans les limites imposées par des conditions légales strictes.

Selon l'Ordonnance relative à l'assistance administrative d'après les conventions contre les doubles impositions, la procédure est la suivante:

L'AFC transmet à l'autorité requérante, en vertu du droit suisse, les informations disponibles qui sont nécessaires pour la mise en œuvre des accords. Elle doit au préalable informer par écrit la personne concernée – ainsi que toute personne qui, en vertu de la loi fédérale sur la procédure administrative (PA), a qualité pour recourir – de la nature et de l'étendue des informations qu'elle entend fournir. Si les personnes légitimées à recourir donnent leur accord écrit à la transmission des informations ou si elles ne répondent pas dans les 30 jours qui suivent la réception de la notification de l'AFC, celle-ci transmettra les informations, soit immédiatement après avoir reçu l'autorisation, soit après échéance du délai. Dans les autres cas, l'AFC rendra une décision. Cette dernière peut faire l'objet d'un recours conformément aux dispositions générales de l'organisation judiciaire fédérale.

Il s'ensuit qu'il est impératif de faire valoir ses droits de recours auprès de l'AFC dans le délai imparti. Comme alternative, l'article 25 LPD prévoit une possibilité de faire valoir ses droits de recours, en dehors de la procédure prescrite dans la CDI CH-USA, pour les transmissions de données qui ont déjà été effectuées.

En résumé, et compte tenu des explications données ci-dessus, il faut retenir qu'une transmission à l'IRS de copies certifiées conformes et d'autres documents est prévue par la CDI CH-USA. Nous conseillons donc aux personnes qui se trouvent dans une telle situation de prendre contact avec l'AFC afin de pouvoir exercer leurs droits dans le délai prescrit et fixer la démarche à suivre. D'autres informations à ce sujet se trouvent au chiffre 1.9.3 du présent rapport d'activités.

À l'heure actuelle, la procédure suit son cours.

1.9.6 Collaboration avec la FINMA concernant les risques opérationnels dans le secteur bancaire

La FINMA nous a consultés dans le courant de l'année 2013 au sujet de la modification de la circulaire 2008/21 «risques opérationnels – banques», respectivement la partie concernant le traitement de données électroniques de clients.

La crise financière et les pertes hors du commun qu'elle a engendrées pour l'économie ont eu pour conséquence une nouvelle approche en matière de risques opérationnels que supportent les prestataires de services financiers. Un débat international a eu lieu à ce sujet débouchant sur l'élaboration de nouvelles régulations, notamment la recommandation d'un taux de fonds propres minimum – afin d'absorber les pertes en cas de crise de liquidités – et des directives en matière de gestion du risque inhérent aux activités numériques du secteur. Les nouvelles exigences ainsi développées n'ont toutefois plus pu être retenues dans les propositions de réglementations bancaires que sont les Accords de Bâle III, ces dernières ayant déjà été mises sur pied avant que des recommandations tangibles n'aient vu le jour. Par conséquent, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a entrepris de les concrétiser dans la circulaire susmentionnée, en l'adaptant aux évolutions qui ont eu lieu.

De surcroît, ladite crise et ses conséquences sur l'économie ont suscité une prise de conscience à grande échelle en matière de sécurité des données électroniques de clients de banques suisses. Les convoitises diverses qu'elles ont éveillées y ont joué un rôle important. La confidentialité de ces données est durement mise à l'épreuve, ce qui a rendu le besoin d'agir urgent. Ainsi, la circulaire énonce dans son annexe 3 «Traitement des données électroniques de clients» les neuf principes de bonne gestion des risques en lien avec la confidentialité des données numériques de particuliers dont les relations commerciales sont administrées en ou de Suisse.

Dans le cadre de notre collaboration, notre travail a notamment porté sur les questions relatives au troisième principe développé par la FINMA «lieu de stockage et accès aux données». Ce principe prévoit dans certains cas une obligation d'anonymisation ou de pseudonymisation des données. L'élément constitutif principal est celui de la sauvegarde de données de clients hors de Suisse ou qui font l'objet d'un accès depuis l'étranger. Le cas échéant, les données d'identification de clients doivent être protégées de manière adéquate, par exemple par chiffrement ou pseudonymisation.

Au vu de ce qui précède, nous constatons une évolution bienvenue en la matière et sommes satisfaits de la collaboration avec la FINMA.

1.10 International

1.10.1 Coopération internationale

La coopération internationale joue un rôle incontournable dans nos activités. L'année 2013 a ainsi été marquée par la poursuite des travaux de modernisation de la Convention 108, des lignes directrices de l'OCDE et du cadre juridique européen. Le renforcement de la coopération entre autorités de protection des données a également été au centre des discussions, notamment au sein de l'Association des autorités francophones de la protection des données, de la Conférence internationale des commissaires à la protection des données et des instances de contrôle communes Schengen, Eurodac et VIS.

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 du Conseil de l'Europe. Ainsi, le projet de modernisation adopté par le comité consultatif de la Convention 108 (T-PD) lors de sa 29e réunion plénière (voir 20e rapport d'activités 2012/2013, ch. 1.9.1) a été transmis à un comité ad'hoc (CAHDATA) composé des représentants gouvernementaux des États membres du Conseil de l'Europe, de l'Uruguay (premier État non européen ayant adhéré à la Convention), des États ayant un statut d'observateur permanent au Conseil de l'Europe et d'un certain nombre d'États tiers susceptibles d'adhérer à la Convention. Des représentants d'organisations internationales, d'organisations non gouvernementales et de l'économie assistent également aux travaux. Le CAHDATA est chargé de finaliser le texte préparé par le T-PD et de préparer un protocole d'amendement à la Convention. Il a tenu une première réunion en 2013 et devrait achever ses travaux d'ici fin 2014.

Pour sa part, le T-PD a examiné le projet de rapport explicatif devant accompagner la Convention révisée et a fixé le cadre des futurs mécanismes de suivi prévus dans le projet de modernisation. Il a également examiné en première lecture une révision de la recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi. Cette révision est rendue nécessaire par les évolutions technologiques et le recours toujours plus fréquent à des technologies de surveillance sur le lieu de travail. Le comité a examiné également un rapport d'expert relatif à l'opportunité de revoir la recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

Le comité est parvenu à la conclusion que vu que la recommandation fait partie intégrante d'accords internationaux contraignants, notamment les accords de Schengen, il n'était pas opportun de la modifier, mais qu'il conviendrait plutôt d'élaborer un nouvel instrument répondant aux exigences actuelles en matière de protection des données dans le cadre des activités de police et de lutte contre la criminalité. Le comité a adopté son programme de travail pour 2014 / 2015. Il se penchera notamment sur la question de l'échange automatique des données à des fins fiscales et financières.

Enfin, le comité a eu un échange de vue sur l'affaire PRISM et les révélations relatives aux activités de la NSA et leurs incidences pour les droits de l'homme et les libertés fondamentales. Dans une lettre adressée au Comité des Ministres du Conseil de l'Europe, le comité estime nécessaire de conduire une réflexion sur le renforcement des mesures visant à mettre en œuvre le cadre juridique applicable aux traitements de données à caractère personnel effectués dans le cadre de programmes de surveillance à des fins de sécurité nationale, afin de garantir à toute personne concernée le respect de ses droits. Il rappelle que ces traitements doivent pouvoir faire l'objet d'un contrôle effectif, indépendant et transparent. Le comité dénonce également l'usage de techniques de surveillance de masse qui pourraient porter gravement atteinte au respect des droits de l'homme et à la démocratie.

Conférence européenne des commissaires à la protection des données

La conférence européenne des commissaires à la protection des données s'est tenue à Lisbonne du 16 au 17 mai 2013 à l'invitation de la commission portugaise de la protection des données. Intitulée «Protecting Privacy: the challenge ahead», la conférence a permis de faire le point sur les réformes en cours du droit de la protection des données au sein de l'Union européenne, du Conseil de l'Europe et de l'OCDE. Nous avons ainsi présenté l'état d'avancement des travaux de modernisation de la Convention 108 et son contenu.

Les commissaires ont également débattu de la manière de rendre plus efficace la protection des données en pratique, notamment sur Internet et les réseaux sociaux. La coopération entre autorités de protection des données, les questions de sécurité des données et le rôle futur des autorités de protection des données au sein de l'Union européenne ont également été abordés.

La conférence a adopté trois résolutions (voir sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale – Conférence européenne des commissaires à la protection des données). La première résolution porte sur l'avenir de la protection des données en Europe. Les commissaires appellent les États européens à renforcer les droits de la personnalité et à soutenir l'adoption d'un cadre juridique assurant

une protection des données effective dans un monde hautement technologique et globalisé.

Ce cadre doit être solide et cohérent et assurer le même niveau de protection dans les secteurs public et privé. Il doit permettre de renforcer les mécanismes de coopération entre les autorités de protection des données, lesquelles doivent être dotées de compétences et de pouvoirs effectifs, ainsi que des ressources humaines et financières suffisantes pour remplir leurs tâches de surveillance de manière indépendante. La deuxième résolution concerne le projet d'accord sur le libre échange entre l'Union européenne et les États-Unis. Les commissaires demandent que cet accord comprenne des dispositions de protection des données. La troisième résolution concerne les nouvelles bases légales devant régir Europol et la nécessité d'assurer un niveau de protection des données adéquat.

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

La 35e Conférence des commissaires à la protection des données et à la vie privée s'est tenue du 13 au 26 septembre 2013 à Varsovie. Réunissant des représentants provenant d'un quarantaine d'États, ainsi que des représentants de l'économie, des administrations, de la société civile et du monde académique, la conférence a permis d'aborder les enjeux actuels en matière de protection des données et notamment l'interopérabilité des outils de transferts internationaux des données, l'accès des autorités publiques aux données, l'éducation numérique, le big data, la cybersécurité, les compétences et le rôle des autorités de protection des données, la problématique des applications mobiles. Cette dernière a fait l'objet d'une déclaration des commissaires sur «l'applification» de la société.

Par cette déclaration, les commissaires s'engagent à veiller à ce que les utilisateurs jouissent d'une meilleure expérience en matière de protection des données et comptent débattre avec les divers intervenants des secteurs public et privé de leurs rôles et responsabilités. Ils rappellent ainsi que les utilisateurs doivent garder la maîtrise des données qui les concernent et ainsi pouvoir décider quelles informations peuvent être communiquées et à quelles fins.

En outre, les développeurs d'applications doivent prendre en considération les exigences de la protection des données dès la conception d'une application. Ils doivent prendre une décision claire concernant les données qu'ils jugent nécessaires au bon fonctionnement de l'application et s'assurer qu'aucune autre donnée n'est collectée sans le consentement éclairé de l'utilisateur. Enfin, ils soulignent que les fournisseurs de systèmes d'exploitation sont également responsables de la protection des données sur leurs plateformes. Les commissaires vont œuvrer

durant l'année 2014 afin d'améliorer la protection des données dans le domaine des applications et reviendront sur cette question lors de leur 36e conférence.

Les commissaires ont adopté plusieurs résolutions (voir sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale – Conférence internationale des commissaires à la protection des données) Dans une résolution, les commissaires invitent les organismes qui font du profilage en particulier:

- à déterminer clairement la nécessité et l'utilisation pratique de chaque activité de profilage et à s'assurer de mettre en place des mesures de sécurité adéquates avant d'entreprendre le profilage;
- à limiter dès l'étape de la conception la quantité de données collectées au niveau nécessaire aux fins licites prévues et à assurer la mises à jour et l'exactitude des données;
- à informer sur les activités de profilage, notamment sur la manière d'établir les profils et sur les finalités poursuivies;
- à s'assurer, en particulier lors de décisions ayant des répercussions juridiques importantes pour des personnes, que celles-ci sont informées de leur droit de consulter et de corriger les données personnelles et de recourir à une intervention humaine s'il y a lieu;
- à s'assurer que toute activité de profilage fait l'objet d'un surveillance appropriée.

Dans une deuxième résolution relative au suivi sur le Web (webtracking) et la protection de la vie privée, les commissaires reconnaissent que le suivi comporte certes certains avantages pour les consommateurs, mais que cette activité pose un risque sans précédent d'atteinte à la vie privée. Il appelle ainsi les parties prenantes:

- à respecter le principe de finalité;
- à informer les utilisateurs du recours à des éléments de suivi et leur permettre d'avoir la maîtrise de ces éléments;
- à s'abstenir d'utiliser des dispositifs de suivi invisibles à des fins autres que la sécurité et le dépistage des fraudes, ou la gestion du réseau;
- à faire preuve de la transparence appropriée au sujet de tous les types de pratiques de suivi sur le Web;
- à offrir aux utilisateurs des outils conviviaux leur permettant de maîtriser de manière adéquate la collecte et l'utilisation de leurs données personnelles;

- à s'abstenir de suivre l'activité en ligne d'enfants ou sur les sites web destinés aux enfants;
- à respecter la vie privée dès la conception et à réaliser une évaluation des facteurs relatifs à la vie privée au début de nouveaux projets;
- à utiliser des techniques réduisant les répercussions sur la vie privée, notamment la dépersonnalisation et l'utilisation de pseudonymes;
- à promouvoir l'adoption de normes techniques visant à conférer aux utilisateurs une meilleure maîtrise.

Une troisième résolution appelle à une amélioration et un renforcement de la transparence, principe essentiel pour permettre aux personnes de prendre des décisions éclairées concernant l'utilisation de leurs données et d'agir en conséquence pour protéger leur vie privée et faire valoir leurs droits. Cette résolution est complétée par une résolution relative à une éducation au numérique pour tous. Le numérique est partie intégrante de notre vie quotidienne. Pour faire face au défi en matière de protection des données, le cadre juridique ne peut à lui seul apporter toutes les réponses et garanties nécessaires. Les commissaires considèrent dès lors indispensable de promouvoir une culture générale du numérique, d'agir ensemble à cet effet avec les acteurs concernés et d'adopter un programme commun, notamment en vue d'une formation continue au numérique.

Rappelant les déclarations (voir notamment la déclaration de Montreux, 13e rapport d'activités 2005 / 2006) et les résolutions adoptées lors des précédentes conférences, les commissaires ont adopté une résolution appelant à l'inscription de la protection des données et de la protection de la vie privée dans le droit international. Aux yeux des commissaires, suite aux révélations d'Edward Snowden, il est de plus en plus urgent de mettre en place un accord juridiquement contraignant sur la protection des données qui garantisse le respect des droits de l'homme lors du traitement de données personnelles tout en tenant compte de façon équilibrée, de la sécurité, des intérêts économiques et de la liberté d'expression.

Enfin, dans deux autres résolutions, l'une sur la coordination de l'application de la loi à l'échelle internationale, l'autre sur l'orientation stratégique de la conférence internationale, les commissaires s'engagent à améliorer et renforcer leur collaboration, notamment pour assurer une coordination des enquêtes transnationales. Un document global et multilatéral mettant en place un cadre pour coordonner les actions internationales en matières de contrôle et d'échange d'informations sera présenté en vue d'adoption à la 36e Conférence qui se tiendra en octobre 2014 à l'Île Maurice.

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

Le groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée s'est essentiellement employé cette année à parachever les directives sur la sécurité et la protection des données. Au terme d'intenses discussions, il a été décidé de maintenir les huit principes fondamentaux déjà établis. Par contre, de nouveaux programmes de gestion de la protection de la vie privée sont prévus, par lesquels les entreprises seront tenues de mettre systématiquement à la disposition des clients et des autorités toutes les informations importantes en matière de protection de la vie privée. Un devoir d'information est introduit en cas de violation de la sécurité des données ou de la protection des données (notification des violations de données). De plus, les critères applicables aux transmissions de données à l'étranger sont définis de manière plus précise, la coopération internationale est renforcée et l'accent est mis sur la sensibilisation et la formation du public. L'incitation à adopter des technologies respectueuses de la vie privée a également été prise en compt. Enfin, le respect de la vie privée est reconnu comme droit fondamental. Le comité des ministres ayant adopté ces nouvelles lignes directrices, le groupe de travail se consacrera prochainement à leur mise en œuvre.

Le rôle des données personnelles dans l'économie a été au cœur des discussions. Du fait de la forte croissance de la numérisation du traitement et du stockage de données personnelles, le cloud computing (informatique en nuage), le big data (datamasse) et l'open data (ouverture des données publiques) sont devenus des thèmes permanents du groupe de travail. Nul ne contestera que la croissance économique future sera indissociable de l'exploitation d'une énorme quantité de données. La protection de la vie privée sera à cet égard d'une importance capitale. Hormis l'État et l'économie, le rôle de l'utilisateur du réseau Internet sera un élément de plus en plus central; en effet, c'est lui qui génère la majeure partie des données personnelles disponibles en ligne. D'autres actions s'imposent afin de compenser le manque de transparence et de protection dans ce contexte surtout. Par ailleurs, étant donné l'énorme volume de données, la question de la sécurité se pose inévitablement. Il en découle aussi un lien avec les lignes directrices de l'OCDE sur la protection des données, récemment mises à jour, et avec les lignes directrices de l'OCDE sur la sécurité, qui doivent encore être révisées.

Il convient aussi de relever que de nombreux États membres sont préoccupés car, estiment-ils, les conditions-cadres relatives à la protection de la vie privée dans le cas de big data, open data, etc. pourraient entraver le développement économique si attendu. Toutefois, l'unanimité règne quant au fait que les méthodes et les processus de traitement des données doivent se conformer aux dispositions en matière de protection des données locales et non le contraire.

Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP) a tenu sa septième conférence et son Assemblée générale du 21 au 22 novembre 2013 à Marrakech. La conférence a réuni des représentants provenant de 25 États de l'espace francophone. Cela a été l'occasion pour les autorités de protection des données de ces États d'échanger sur les questions qui les interpellent. Elles ont ainsi fait le point sur les développements législatifs en cours au plan national et international dans les différentes régions du monde. Elles ont abordé la question de la défense des libertés sur Internet, de la place des appareils et des services mobiles dans la société et des défis qu'ils entraînent pour les droits et libertés fondamentales. Elles ont également échangé sur leur gestion des communications externes et leur politique médiatique, ainsi que sur l'exercice de leurs compétences, notamment de leur pouvoir de contrôle.

Lors de l'Assemblée générale, les autorités de protection des données de l'espace francophone ont réélu M. Jean Chartier (Québec) à la présidence. M. Jean-Philippe Walter, préposé fédéral suppléant a été réélu à la vice-présidence au côté de Mme Marguerite Ouedraogo (Burkina Faso). Mme Isabelle Falquier-Pierrotin est pour sa part réélue au poste de secrétaire générale.

L'Assemblée a en outre adopté 3 résolutions (voir sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale – AFADPD). La première vise à assurer une plus grande transparence des pratiques de collecte des donnés personnelles par les autorités étatiques et recommandent aux gouvernements des États de l'Organisation internationale de la francophonie de soutenir l'adoption aux Nations Unies d'un instrument juridique contraignant de protection des données et à ceux qui ont adopté une législation de protection des données de demander l'adhésion à la Convention 108 et son protocole additionnel.

Une deuxième résolution porte sur l'éducation au numérique. Les autorités francophones s'engagent à «continuer à promouvoir une utilisation respectueuse et responsable des technologies du monde numérique auprès des citoyens et des organisations publiques et privées» et à «encourager une formation au numérique tout au long de la vie et accessible à tous car il est nécessaire, dans un monde où les technologies évoluent très rapidement, de donner aux personnes des moyens pour devenir des acteurs responsables et égaux face au numérique.»

La troisième résolution concerne l'adoption d'un protocole de coopération entre les autorités membres de l'AFAPD et la mise en place d'une procédure d'encadrement des transferts de données dans l'espace francophone au moyen, notamment, de règles contraignantes d'entreprises (RCE). Ces règles offrent plusieurs avantages. En

particulier, elles permettent de garantir un niveau élevé de protection des données. Cet outil prévoit le respect des principes fondamentaux de protection des données sous forme de codes de conduite internes à l'entreprise et de mécanismes de mise en œuvre (conseiller à la protection des données, procédure d'audit, formation, gestion des plaintes).

Le PFPDT ne pourra à l'heure actuelle pas approuver ces règles contraignantes. Toutefois, comme il le fait pour les RCE européens, il pourra reconnaître des RCE ayant été approuvées par d'autres autorités de protection des données comme offrant des garanties suffisantes lors du transfert de données à l'étranger.

Groupe de travail «Border, Travel & Law Enforcement»

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

Le sous-groupe de travail a en particulier préparé un avis sur le 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 d'États 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 a suivi avec attention la création d'un cadre européen pour la communication des données PNR aux États tiers et pour l'utilisation des données PNR à des fins répressives. Il suit également la révision du cadre juridique de protection des données de l'Union Européenne instaurée par le Traité de Lisbonne. Le sous-groupe élabore une opinion sur le principe de nécessité en matière de protection des données. Enfin, depuis l'éclatement de l'affaire Snowden, le sous-groupe discute activement du programme PRISM et d'autres programmes similaires.

Groupe de coordination du contrôle du SIS II

Le 11 juin 2013 a eu lieu la première réunion officielle du groupe de coordination du SIS II qui a remplacé l'autorité de contrôle commune Schengen (ACC) suite à l'entrée en vigueur du SIS II le 9 avril 2013. Le groupe de coordination SIS II est constitué de la même manière que celui chargé du contrôle d'Eurodac et de VIS et se compose également du Commissaire européen pour la protection des données et des autorités nationales de protection des données. Une deuxième séance s'est tenue le 17 octobre 2013.

Lors de ces réunions, le groupe a adopté son règlement interne, élu sa présidente et son vice-président et adopté son nouveau programme de travail qui reprend en grande partie celui des travaux initiés par l'ACC. Il a été informé du bon déroulement du processus de migration du SIS I+ vers le SIS II, qui est devenu opérationnel le 9 avril 2013, ainsi que de la campagne d'information par la Commission.

Lors de la première séance du groupe, l'autorité de protection des données danoise a informé que le N-SIS danois avait été victime de hacking. Suite à cette information, un courrier a été préparé et toutes les autorités de protection des données l'ont adressé à leur Bureau SIRENE national afin que ce dernier s'assure que toutes les mesures de sécurité nécessaires ont été mises en place et qu'aucun incident similaire n'est survenu. Enfin, le groupe a créé un sous-groupe chargé d'élaborer un document concernant l'inspection des alertes SIS II, VIS et EURODAC.

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 des développements en cours et des activités de l'ACC, 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 25e réunion du groupe de travail européen sur le traitement de cas relevant de la protection des données («Case Handling Workshop»), s'est tenue à Sarajevo du 2 au 3 octobre 2013. Le groupe de travail, constitué de représentants de 29 autorités nationales de protection des données s'est concentré sur plusieurs sujets. Le groupe a ainsi premièrement abordé la problématique des réseaux sociaux et d'internet. Il en ressort qu'il faut impérativement sensibiliser le public aux dangers de ces réseaux et de les responsabiliser; plusieurs autorités de protection des données ont rédigé un guide à l'intention du jeune public. De son côté, le PFPDT soutient l'initiative de la campagne multimédia «NetLa – mes données m'appartiennent» destinée aux enfants et aux jeunes (voir notre 18e rapport d'activités 2010/2011, ch. 3.3 et www.netla.ch).

Dans un deuxième temps, la discussion a porté sur les nouveaux défis soulevés par l'utilisation de la téléphonie mobile dans le domaine de la protection des données, notamment l'utilisation de la messagerie «WhatsApp». Enfin, le marketing direct, l'utilisation de données biométriques ainsi que la vidéosurveillance dans le secteur public et privé ont été thématisés et illustrés à l'aide des divers cas concrets tirés de la pratique des différentes autorités de protection des données. L'autorité de protection des données bosniaque publiera prochainement un manuel sur tous les sujets abordés lors de cette réunion.

Visite de la Commissaire géorgienne à la protection des données

À la demande du DFAE, nous avons reçu la commissaire géorgienne à la protection des données ainsi que la responsable du département des relations internationales et de la communication pour une journée d'information et d'échange sur nos pratiques en matière de conseil et de contrôle.

Le DFAE a organisé en décembre 2013 une visite diplomatique de la commissaire géorgienne à la protection des données. La loi géorgienne sur la protection des données est entrée en vigueur au printemps 2013 et la commissaire a pris ses fonctions durant l'été. Son service, qui compte 14 personnes, est en cours de développement. Ses activités se concentrent sur le conseil et des procédures de contrôle auprès du secteur privé pourront être entreprises dès l'année 2016.

Dans ce cadre, la commissaire tient à rencontrer différentes autorités de protection des données en Europe pour s'informer sur leur organisation et leur fonctionnement. Accompagnée de la responsable du département des relations internationales et de la communication, elle a choisi notre autorité pour sa première visite du fait des très bonnes relations diplomatiques entre la Suisse et la Géorgie.

Une journée d'échange a ainsi eu lieu dans nos locaux. Nous avons accueilli officiellement la délégation géorgienne, accompagnée du conseiller à la protection des données du DFAE et avons présenté notre organisation interne. Nous avons ensuite détaillé nos tâches en illustrant nos propos avec différents exemples tirés de nos activités de conseil et de contrôle. Nous avons également présenté notre méthode de travail, les outils et l'infrastructure à notre disposition et finalement nos actions en matière de sensibilisation à la protection des données.

2. Principe de la transparence

2.1 Demandes d'accès

2.1.1 Départements et offices fédéraux

Selon les chiffres qui nous ont été communiqués, 469 demandes d'accès ont été déposées auprès des autorités fédérales en 2013. Dans 218 cas, les autorités ont accordé un accès complet et dans 103 cas un accès partiel. Dans 122 cas, l'accès aux documents a été totalement refusé. 18 demandes d'accès ont été retirées; dans plus de la moitié de ces cas, le retrait a été motivé par le montant des émoluments requis par les autorités. À la fin de l'année, huit cas étaient encore en suspens.

Pour ce qui est du nombre total des demandes d'accès et de la pratique des autorités à ce sujet, les chiffres donnent une image générale de stabilité par rapport aux années précédentes. Ces résultats indiquent que la loi sur la transparence (LTrans) est désormais considérée par les particuliers et les professionnels des médias comme un moyen utile et efficace pour obtenir des informations. Nous espérons néanmoins que la visibilité et l'utilité de la LTrans poursuivront leur progression.

Pour ce qui est des offices, c'est l'OFSP qui a reçu le plus grand nombre de demandes d'accès pour l'année 2013 (33 demandes), suivi de l'OFAG (30), de l'IFSN (26) et de l'ODM (24). Parmi les départements, le DETEC (100), le DFI (92) et le DFAE (73) sont en tête. Le DFAE semble parmi les plus favorables au principe de la transparence avec, sur un total de 73 demandes d'accès, 63 réponses entièrement positives; ce département a accordé un accès partiel à cinq autres demandes et a refusé entièrement l'accès aux informations demandées dans cinq autres cas seulement. Sur 71 autorités, 19 nous ont informés qu'elles n'avaient reçu aucune demande d'accès pour l'année 2013. Au cours de l'année sous revue, le Préposé lui-même a reçu 14 demandes d'accès: il a accordé dix accès entiers, trois accès partiels et prononcé un refus complet.

Comme au cours de l'année précédente, les émoluments demandés par les autorités sont demeurés relativement modestes avec un total de CHF 6502,50 (année précédente 6300 francs). Il est intéressant de noter à ce propos que trois départements et la Chancellerie fédérale n'ont prélevé aucun émolument, alors que quatre autres départements ont partiellement facturé leur temps de travail aux demandeurs. Sur les CHF 6502,50 d'émoluments facturés, presque la moitié l'ont été par l'Inspection fédérale de la sécurité nucléaire IFSN. Bien que seulement 2015 francs parmi ces émoluments soient à mettre au compte des unités de l'administration fédérale centrale, la Conférence des secrétaires généraux (CSG) a estimé nécessaire de mettre sur pied un groupe de travail chargé d'élaborer

des directives sur le prélèvement d'émoluments pour les demandes d'accès conformément à la LTrans (voir chiffre 2.6.1 du présent rapport d'activités).

En ce qui concerne la charge de travail occasionnée par les demandes d'accès, nous soulignons le fait que les autorités ne sont pas tenues de noter les heures qu'elles y consacrent. En outre, il n'existe aucune directive sur la saisie uniforme du temps de travail qui soit applicable à l'ensemble de l'administration fédérale. Ces données, qui nous sont transmises sur une base volontaire, ne sont pertinentes que dans une certaine mesure. Selon ces chiffres donc, la charge de travail a diminué, cela pour la première fois (2010: 815 heures; 2011: 1519 heures; 2012: 2155 heures; 2013: 1707). Les heures consacrées à la participation à des procédures de médiation ont par contre augmenté de plus de 60 pour cent: de 480 heures en 2012, elles sont passées à 778 heures en 2013.

2.1.2 Services parlementaires

Les Services parlementaires n'ont reçu aucune demande en 2013.

2.1.3 Ministère public de la Confédération

Pour l'année 2013, le Ministère public de la Confédération nous a informés n'avoir reçu qu'une demande d'accès pour laquelle il a prononcé un refus complet.

2.2 Demandes en médiation

En 2013, nous avons reçu un total de 76 demandes en médiation (2012: 78). Contrairement à l'année précédente, la plupart d'entre elles ont été déposées par des particuliers (27 demandes), suivis de très près par les journalistes (24). Ces chiffres permettent de faire les remarques suivantes: sur un total de 225 demandes, l'administration fédérale avait entièrement refusé l'accès 122 fois et l'avait accordé partiellement 103 fois. Suite à ces refus complets et partiels, 76 demandes en médiation ont été déposées chez nous. Cela signifie qu'environ 30 pour cent des accès entièrement ou partiellement refusés ont été suivis d'une demande en médiation.

Au total, 81 procédures en médiation ont été menées à terme durant l'année 2013. Parmi celles-ci, 31 avaient été déposées en 2013, 30 dataient de 2012 et 17 de 2011. Dans 16 cas, nous avons trouvé un accord consensuel avec les parties impliquées. Nous avons émis des recommandations dans 38 cas, faute d' arrangement. 13 demandes en médiation ont été retirées et dans sept cas, les conditions d'application de la LTrans n'étaient pas données. Dans quatre cas, la demande en médiation n'a pas été remise dans les délais.

En raison de la sous-dotation persistante en personnel, les demandeurs continuent d'attendre plus longtemps que les 30 jours prévus par la loi pour que la procédure de médiation soit engagée.

2.3 Procédures de médiation closes

2.3.1 Recommandations

Les recommandations émises au cours de l'année 2013 concernant la LTrans sont brièvement résumées ci-dessous. Elles peuvent être consultées en version intégrale (dans leur majorité en allemand) sur notre site internet www.leprepose.ch à la rubrique Principe de la transparence – Recommandations – 2013.

1. Recommandation armasuisse / Convention d'utilisation de l'aérodrome militaire de Buochs (25 janvier 2013)

Le demandeur a requis auprès d'armasuisse l'accès à la convention relative à l'utilisation conjointe civile de l'aérodrome militaire de Buochs, entre armasuisse et l'Airport Buochs AG, y compris annexes et appendices. armasuisse a prononcé un refus complet d'accès aux documents en invoquant la garantie de la libre formation de l'opinion et de la volonté d'une autorité ainsi que la protection des secrets professionnels, d'affaires et de fabrication.

En dépit de plusieurs rappels écrits et téléphoniques du Préposé, armasuisse n'a pas remis d'avis motivé et détaillé ni délivré les documents officiels demandés.

Dans sa recommandation, le Préposé a conclu que par son manquement, armasuisse avait violé son devoir de collaboration. Étant donné que le fardeau de la preuve destiné à renverser la présomption de libre accès aux documents officiels incombe aux autorités, le Préposé a estimé que la preuve d'une situation d'exception permettant de justifier un refus d'accès n'était pas fournie; il a donc recommandé l'accès aux documents demandés sous réserve d'éventuelles dispositions d'exception de la LTrans.

2. Recommandation armasuisse / Documents concernant le projet de vente d'un terrain (28 janvier 2013)

Les demandeurs avaient déposé auprès d'armasuisse une offre d'achat pour un terrain situé sur la commune de X. Peu après, armasuisse les a informés que le terrain en question n'était pas en vente, contrairement à l'appel d'offres. Les demandeurs ont donc requis des copies de tous les documents officiels en relation avec cette vente. En réponse, armasuisse a informé les demandeurs des motifs qui avaient conduit à ce changement de politique et s'est déclaré dans tous les cas prêt à leur permettre de prendre connaissance sur place d'une partie des documents. Dans une lettre ultérieure, les demandeurs ont confirmé leur demande d'accès et souligné, à l'attention d'armasuisse, qu'en tant que demandeurs, ils avaient le choix d'obtenir des copies ou un simple accès sur place.

En dépit de plusieurs rappels écrits et téléphoniques, armasuisse n'a pas donné suite à la demande du Préposé visant la remise d'un avis motivé et détaillé et la délivrance des documents officiels demandés.

Dans sa recommandation, le Préposé a conclu que par son manquement, armasuisse avait violé son devoir de collaboration. Étant donné que le fardeau de la preuve destiné à renverser la présomption de libre accès aux documents officiels incombe aux autorités, le Préposé a estimé que la preuve d'une situation d'exception permettant de justifier un refus d'accès ou de n'accorder qu'un accès partiel n'était pas fournie. Sans compter qu'il ne comprenait pas pourquoi armasuisse n'avait envisagé que la possibilité d'une consultation (partielle) sur place. Il a donc recommandé de faire parvenir aux demandeurs sous forme de copies les documents demandés sous réserve d'éventuelles dispositions d'exception de la LTrans.

3. Recommandation SECO / Comptes de pertes et profits et bilans – Contributions aux frais d'exécution (20 février 2013)

Le demandeur a requis auprès du Secrétariat d'État à l'économie (SECO) l'accès aux comptes de profit et pertes et aux bilans des commissions paritaires; conformément à une clause figurant dans la déclaration d'application générale de leurs conventions collectives de travail, ces commissions doivent remettre lesdits documents au SECO.

Le SECO a refusé l'accès à ces documents en invoquant le fait que la loi ne prévoit pas de droit autonome d'un tiers à leur consultation. En outre, toujours de l'avis du SECO, les documents demandés renferment des secrets professionnels et leur divulgation aurait aussi porté atteinte à la sphère privée de tiers.

Dans sa recommandation, le Préposé est parvenu à la conclusion que les comptes des profits et pertes et les bilans ne contenaient pas de secrets professionnels car il n'y avait pas situation de concurrence. Concernant les données personnelles, il a recommandé l'accès à celles faisant l'objet d'un intérêt public prépondérant.

4. Recommandation DDPS / Rapport Constatations Révision des caisses de la brigade d'infanterie de montagne 12 (4 mars 2013)

Le demandeur a requis auprès du Département fédéral de la défense, de la protection de la population et des sports (DDPS) l'accès à tous les documents en relation avec une enquête interne menée au DDPS suite à des irrégularités financières touchant l'utilisation de fonds de sponsoring par une unité militaire. Le DDPS a refusé cet accès en invoquant entre autres le fait que les documents renfermaient des données personnelles concernant l'ancien commandant de brigade, données que l'on ne pouvait pas anonymiser. De plus, le DDPS ne voyait pas d'intérêt public supérieur lié aux informations recherchées. Il faisait en outre valoir que la protection

de la vie privée, en tant que droit fondamental protégé par la Constitution et la CEDH, primait sur le droit à l'accès à des informations officielles, droit qui selon le DDPS n'est protégé qu'indirectement par la Constitution.

Dans sa recommandation, le Préposé a retenu que d'une manière générale, les documents officiels revêtaient déjà un intérêt public important du fait de l'esprit et du but de la LTrans. Il a en outre estimé que le fait qu'il pourrait s'agir d'une utilisation irrégulière de fonds de sponsoring privés par un employé de la Confédération haut placé et occupant une fonction spéciale plaide en faveur d'un intérêt public particulier. Pour conclure, le Préposé a précisé que la pesée des intérêts entre l'intérêt public à l'accès aux documents et l'intérêt de la personne concernée à voir sa sphère privée protégée devait pencher en faveur de l'accès. Il a donc demandé au DDPS d'auditionner la personne concernée avant une éventuelle autorisation d'accès et de masquer les données personnelles sensibles figurant dans les documents.

5. Recommandation IFSN / Valeurs de mesures issues de l'instrumentation des cheminées de la Centrale nucléaire de Mühleberg (18 mars 2013)

Le demandeur a requis auprès de l'Inspection fédérale de la sécurité nucléaire (IFSN) l'accès aux données recueillies en continu concernant l'activité de l'air évacué par la centrale nucléaire de Mühleberg pour les périodes de juillet à août 2012 ainsi que, à titre comparatif, de juillet à septembre 2011. L'IFSN a refusé l'accès à des données au motif, notamment, que les valeurs de mesure requises n'étaient pas disponibles sous une forme qui permettrait d'établir un document officiel, par un procédé électronique simple, à partir d'informations enregistrées. En outre, l'IFSN relevait que les valeurs de mesure demandées, qui lui sont remises exclusivement en vue d'une intervention d'urgence, avaient été effacées automatiquement et définitivement au bout de 30 jours conformément aux dispositions du règlement d'exploitation en vigueur.

Comme l'a relevé le Préposé dans sa recommandation, il apparaît clairement – sur la base de la confirmation écrite de l'IFSN à propos de la suppression effective des données ainsi de la consultation du règlement d'exploitation mentionné – que les valeurs de mesures demandées étaient déjà entièrement effacées au plus tard au moment de l'ouverture de la procédure de médiation. Par conséquent, elles n'étaient plus enregistrées et de ce fait n'étaient plus en possession de l'IFSN. Le Préposé a néanmoins souligné qu'à son avis, l'IFSN aurait dû sauvegarder les données qui étaient encore en sa possession au moment où la demande d'accès a été reçue, et ce jusqu'à ce que la procédure d'accès soit close.

Il a également examiné la question de savoir si l'IFSN aurait pu établir, par un traitement informatisé simple, un document officiel à partir d'informations enregistrées; il s'est limité à cet égard à constater que tel devrait être le cas dès lors qu'un seul collaborateur auprès de l'autorité concernée pourrait, sans contrainte excessive, convertir les données disponibles en document officiel à l'aide du logiciel adapté. En définitive, le Préposé a approuvé le refus d'accès de l'IFSN en raison de l'effacement effectif des données demandées.

6. Recommandation OFJ / Actes d'une procédure judiciaire (21 mars 2013)

Le demandeur a adressé une demande d'accès à l'Office fédéral de la justice (OFJ) concernant l'affaire Portmann c. Suisse auprès de la Cour européenne de droits de l'homme (CEDH). Le demandeur a requis l'accès à la requête et aux observations du requérant ainsi qu'aux observations déposées par la Suisse.

L'autorité a informé le demandeur qu'elle refusait d'accorder l'accès aux documents requis au motif que la loi n'était en l'espèce pas applicable car une procédure était pendante devant la Grande Chambre.

Le Préposé a constaté que le collège de cinq juges de la Grande Chambre a rejeté la demande de renvoi, de sorte que l'arrêt rendu le 11 octobre 2011 par la deuxième section de la CEDH est dès lors devenu définitif le 8 mars 2012 en vertu de l'article 44, §2, let.C, de la Convention européenne des droits de l'homme.

Les documents requis sont des actes rédigés et déposés par les parties à la cause Portmann c. Suisse dans le cadre de la procédure judiciaire par-devant la CEDH. Par conséquent, le Préposé est arrivé à la conclusion que ces documents étaient dès lors exclus du champ d'application matériel de la LTrans, pendant et après la fin de la procédure devant la CEDH.

7. Recommandation OFJ / Procédure de recrutement et de sélection des candidats au poste de juge auprès de la CEDH (25 mars 2013)

Le demandeur a adressé une demande d'accès à l'Office fédéral de la justice (OFJ) concernant la mise au concours, en 2010, du poste de juge au titre de la Suisse auprès de la Cour européenne des droits de l'homme (CEDH), ainsi que la procédure de recrutement et de sélection des trois candidats présentés par la Suisse à l'Assemblée parlementaire du Conseil de l'Europe en vue de leur élection.

L'OFJ a partiellement admis la demande d'accès et a communiqué au demandeur certaines informations concernant le processus de recrutement et de sélection: à savoir le nombre de candidats ayant postulé ainsi que la liste des trois noms transmis au panel consultatif d'experts pour l'élection des juges à la CEDH. L'autorité a par

contre explicitement refusé de divulguer la liste des candidats et le classement des candidats.

Le Préposé n'a que très partiellement admis les griefs du demandeur et est arrivé à la conclusion qu'il incombe à l'OFJ de transmettre au demandeur uniquement une liste des documents officiels concernés, et d'inviter ce dernier à préciser sa deuxième demande et sur cette base d'apprécier si l'accès aux documents requis peut être accordé.

8. Recommandation CNPT/ Applicabilité de la LTrans à la CNPT (11 avril 2013)

Le demandeur a déposé une demande auprès de la Commission nationale de prévention de la torture (CNPT) et a requis l'accès à la correspondance de la CNPT avec le Comité européen pour la prévention de la torture (CPT) depuis 2010 et à la correspondance de la CNPT avec le CPT depuis 2010 au sujet de la grève de la faim de Bernard Rappaz.

La CNPT a communiqué au demandeur par courrier électronique qu'elle refusait d'accorder l'accès aux documents requis au motif que ceux-ci étaient confidentiels. Dans sa prise de position à l'attention du Préposé, la CNPT a de plus allégué qu'elle n'était pas soumise à la LTrans.

Le Préposé a constaté que la CNPT est mentionnée dans l'annexe 1 de l'ordonnance sur l'organisation du gouvernement et de l'administration, en tant qu'unité administrative décentralisée de l'administration fédérale, à savoir du Département fédéral de justice et police. Le Préposé est par conséquent parvenu à la conclusion que la CNPT est soumise à la LTrans et qu'il appartient par conséquent à l'autorité de reconsidérer sa prise de position et d'apprécier si l'accès aux documents requis peut être accordé et, le cas échéant, dans quelle mesure.

9. Recommandation IFSN / Rapport sur la résistance sismique de la centrale de Mühleberg (10 avril 2013)

Le demandeur a déposé une demande d'accès auprès de l'Inspection fédérale de la sécurité nucléaire (IFSN) et a requis l'accès à deux rapports portant sur la résistance sismique des structures de la centrale de Mühleberg. L'IFSN lui en a refusé l'accès au motif qu'il avait simultanément demandé l'accès aux mêmes documents en tant que partie dans une procédure administrative cantonale. Toutefois, aucune décision n'avait été encore prise sur sa demande de verser les documents visés au dossier de procédure. L'IFSN a en outre estimé que certes les documents d'une procédure administrative de première instance étaient en principe soumis au droit d'accès, mais cela seulement lorsque la décision correspondante était définitive et exécutoire. Dans sa recommandation, le Préposé a constaté que les documents

requis ne faisaient en effet, au moment où la recommandation était émise, de toute évidence pas (encore) partie du dossier de procédure cantonale mais que la question de leur intégration dans la procédure en cours n'avait toutefois encore été tranchée. Il a de ce fait recommandé d'ajourner l'accès jusqu'à la décision définitive de l'autorité cantonale sur l'intégration des rapports en question dans le dossier de procédure.

10. Recommandation OFAC / Documents relatifs au profilage des passagers dans les aéroports suisses (15 avril 2013)

Le demandeur a requis auprès de l'Office fédéral de l'aviation civile (OFAC) l'accès aux projets et directives concernant le profilage des passagers dans les aéroports suisses. L'OFAC a rendu une réponse négative en invoquant notamment le fait qu'octroyer un accès à ces documents menacerait gravement la sécurité intérieure et extérieure de la Suisse. Une fois informés des mesures concrètes de profilage, les terroristes potentiels n'auraient aucune difficulté à les contourner. Donc, pour cette raison, le document en question était classé confidentiel.

Dans sa recommandation, le Préposé a établi que sur le principe, il partageait la position de l'OFAC selon laquelle un accès aux documents concernant les mesures concrètes de profilage constituait un danger pour la sécurité aérienne. Mais, faisant référence aux documents à évaluer, il est toutefois parvenu à la conclusion que ces derniers étaient formulés de façon très générale et de ce fait ne contenait aucune information qui aurait pour conséquence une mise en danger de la sécurité s'ils étaient divulgués.

En définitive, le Préposé a recommandé l'accès aux documents demandés après annulation de leur classification.

11. Recommandation DFF / Adaptation du droit suisse en matière fiscale aux standards de l'OCDE (27 mai 2013)

Le demandeur a requis auprès du Département fédéral des finances (DFF) l'accès à un rapport (annexes comprises) concernant le rôle de l'administration dans l'adaptation au standard de l'OCDE des conditions d'octroi de l'entraide administrative en matière fiscale. Le DFF a refusé l'accès aux documents demandés au motif qu'il s'agissait d'un rapport rédigé sur la base d'une décision rendue par le Conseil fédéral et destiné à ce dernier, donc que ce rapport faisait partie intégrante d'une affaire du Conseil fédéral et, à ce titre, n'était pas soumis à la LTrans. De plus, jusqu'à ce que la cheffe du département signe la note de discussion, le rapport n'était qu'un projet et ne constituait donc pas un document officiel.

Ainsi, de par sa genèse et son statut du point de vue du droit de la procédure, le rapport ne se distinguait pas de la note de discussion à laquelle il avait été joint

comme annexe. De plus, le DFF estimait qu'objectivement parlant, il fallait considérer le rapport comme appartenant à la procédure de co-rapport, donc comme n'étant pas soumis à la LTrans. Dans sa recommandation, le Préposé a considéré que le rapport constituait un document officiel ayant atteint son stade définitif qui ne doit pas être considéré comme faisant partie de la note de discussion, mais en constitue l'annexe. De plus, de l'avis du Préposé, le document n'équivaut pas à un document afférent à la procédure de co-rapport. Le Préposé a donc recommandé au DFF de faire parvenir au demandeur une liste de tous les documents annexés au rapport et de le prier instamment de préciser sa demande à leur sujet.

12. Recommandation SECO / Dossier d'enquête concernant l'exportation de grenades à main vers la Syrie (28 mai 2013)

Le demandeur a requis auprès du Secrétariat d'État à l'économie (SECO) l'accès au dossier d'enquête concernant des grenades à main exportées par la Suisse. Le SECO a refusé l'accès aux documents demandés entre autres au motif que ces documents ne tombaient pas dans le champ d'application personnel de la LTrans et constituaient des pièces afférentes à la procédure de co-rapport.

Dans sa recommandation, le Préposé a conclu que les documents demandés doivent être qualifiés de documents du Conseil fédéral et font partie de la procédure de co-rapport, raison pour laquelle leur accès doit être refusé. Le Préposé a estimé que l'accès aux autres documents doit aussi être refusé pour des raisons tenant à la sécurité du pays et aux relations extérieures. Enfin, le Préposé a souligné qu'il est impossible de faire valoir un droit pour ce qui est de deux documents car ils ont été établis par la Commission de gestion du Conseil national et sont destinés au Conseil fédéral, et qu'il y a donc là un état de fait spécifique à la LTrans. La loi sur le parlement établit en effet que les délibérations et les documents de séance des commissions sont confidentiels. Concernant deux notes diplomatiques, le Préposé a conclu par contre que leur accès devait être accordé car le SECO n'avait pas de preuve légalement suffisante pour invoquer une exception à la LTrans.

13. Recommandation IFSN / Documents relatifs à un incendie et à une inondation à l'intérieur de la Centrale de Mühleberg (27 juin 2013)

Le demandeur a requis auprès de l'Inspection fédérale de la sécurité nucléaire (IFSN) l'accès à certains documents concernant un incendie et une inondation à l'intérieur de la Centrale de Mühleberg. L'IFSN lui en a refusé l'accès en invoquant un risque possible pour la sécurité intérieure, faisant du reste valoir le fait que les documents en question étaient classés confidentiels. L'IFSN a par ailleurs relevé que le demandeur avait déjà tenté, dans le cadre d'une procédure administrative, d'obtenir l'accès aux mêmes documents à titre d'opposant en faisant valoir son

droit de consulter les dossiers. Le Tribunal administratif fédéral (TAF) avait cependant rejeté la demande d'accès dans une décision intermédiaire du 8 décembre 2010.

Dans sa recommandation, le Préposé a établi que la question de la pertinence des documents en matière de sécurité avait déjà été examinée par le TAF dans le cadre de la procédure administrative mentionnée et qu'il y avait été répondu positivement. Il a donc estimé que rien ne justifie une nouvelle appréciation en vue d'un éventuel accès et s'est joint à l'appréciation du TAF quant à l'évaluation de la sécurité. Il a recommandé en définitive à l'IFSN de s'en tenir à sa prise de position négative.

14. Recommandation SUVA / Entreprises de location de services soumises à une CCT (4 juillet 2013)

Le demandeur a déposé auprès de la Caisse nationale d'assurance en cas d'accidents (SUVA) une demande et requis la liste de toutes les entreprises de location de services assurées auprès de la SUVA dans la classe 70C, qui paient par an un total de salaires de 1 200 000 francs au moins pour les employés temporaires et qui, de ce fait, tombent sous le coup des conventions collectives de travail (CCT) «Location de services» déclarées de force obligatoire. La SUVA a refusé de livrer les renseignements demandés en invoquant une prescription de protection des données figurant dans la loi sur l'assurance-accident (LAA) et interdisant la communication de données personnelles à des tiers non autorisés et qui l'emporterait sur la LTrans en tant que disposition spéciale.

Dans sa recommandation, le Préposé a constaté que ni la norme relative au devoir de discrétion prévue dans la législation générale en matière d'assurances sociales, ni les dérogations concrètes qui en découlent ne priment sur la LTrans en tant que dispositions spéciales. Quant à l'examen de l'accessibilité des informations demandées conformément à la LTrans, le Préposé a conclu que ce type de liste ne peut certes pas être rendu anonyme, mais qu'il y a un intérêt public prépondérant à la communication du nom des entreprises qui sont soumises à la CCT «Location de services». Il a donc recommandé à la SUVA de communiquer la liste demandée.

15. Recommandation OFAG / Extraits du système de gestion des documents (8 juillet 2013)

La demanderesse a requis auprès de l'Office fédéral de l'agriculture (OFAG) l'accès à trois extraits du système de gestion des documents concernant les procédures d'homologation de trois produits phytosanitaires de deux différentes entreprises détentrices d'une autorisation. L'OFAG a refusé l'accès sous forme anonymisée sans audition des entreprises concernées au motif que les listes de documents contenaient des données personnelles relatives aux sociétés de fabrication et qu'elles ne pouvaient plus être rendues anonymes du fait de la publication du

répertoire des produits phytosanitaires par l'OFAG. Par ailleurs, l'office a estimé qu'une audition des détentrices d'une autorisation permettrait d'indiquer à l'OFAG les secrets d'affaires et de fabrication éventuellement contenus dans les listes de documents.

Dans sa recommandation, le Préposé a rejeté l'existence d'un devoir d'audition et d'un devoir d'anonymisation de l'OFAG. Il a également rejeté l'existence de secrets d'affaires et de secrets professionnels dans les listes de documents à évaluer. Il a par contre reconnu la présence d'un intérêt public prépondérant à un accès à ces documents en raison, d'une part, de la situation particulière entre les détentrices des autorisations et la Confédération et, d'autre part, en raison de la large couverture médiatique récemment suscitée par l'utilisation des produits phytosanitaires. Il a donc recommandé un accès sans réserve aux listes de documents demandés et la renonciation à tout émolument.

16. Recommandation OFAG / Listes des destinataires de la contribution pour le lait transformé en fromage et pour le non-ensilage (7 août 2013)

Le demandeur a requis auprès de l'Office fédéral de l'agriculture (OFAG) les listes des destinataires de la contribution pour le lait transformé en fromage et pour le non-ensilage, allouée de 2006 et 2011. L'OFAG a refusé l'accès à cette liste de onze pages au motif que tant les noms des destinataires des contributions que le montant de la contribution constituent des données personnelles et qu'aucun intérêt public prépondérant ne justifie leur consultation. Ce n'est qu'en procédure de médiation que l'OFAG a communiqué qu'en cas d'audition, il faudrait contacter 2500 personnes et que cette démarche ainsi que les frais d'envoi s'élèveraient à un total de 275 000 francs. Au cours de la procédure de médiation, le demandeur et l'OFAG se sont accordés sur le fait que la demande d'accès ne porterait que sur les 40 principaux destinataires des listes des années 2006 à 2012. Au terme de la procédure de conciliation, l'OFAG a requis en outre un émolument de 1800 francs pour l'établissement de cette liste.

Dans sa recommandation, le Préposé a qualifié de données personnelles tant le nom des destinataires des contributions que le montant même des contributions; la communication de ces données ne porte toutefois atteinte, si tel est le cas, que de manière minime à la sphère privée des destinataires. Il a conclu que dans le cas présent, l'accès illimité aux listes peut être accordé même sans audition des destinataires des contributions, d'autant plus qu'il n'existe aucune exception conformément à la LTrans. Pour ce qui est des émoluments, le Préposé a désapprouvé tant la perception d'émoluments pour l'audition (frais administratifs et frais d'envoi) que pour l'établissement des listes (frais administratifs). Par la suite, l'OFAG a publié sur son site web la liste intitulée «Zulagenbezüger mit > CHF 1 Mio. pro Jahr von 2006 – 2012» (uniquement en allemand).

17. Recommandation AFC / Données relatives à l'impôt fédéral direct (22 août 2013)

Le demandeur a requis auprès de l'Administration fédérale des contributions (AFC) les données relatives à l'impôt fédéral direct à partir de l'année 1990, sous forme d'une base de données structurée.

Le Préposé a constaté que selon les informations fournies par l'AFC, les opérations nécessaires à l'établissement du document requis impliquaient la réalisation d'opérations supplémentaires de programmation complexes, à savoir l'introduction manuelle par un collaborateur spécialisé de nouvelles requêtes dans les différentes bases de données concernées.

Le Préposé est arrivé à la conclusion qu'au vu de la complexité, de l'ampleur et de la durée des opérations nécessaires à l'établissement du document requis, il ne s'agit en l'espèce pas d'un traitement informatisé simple au sens de la LTrans. Dès lors, le Préposé a finalement conclu que l'AFC n'avait pas l'obligation d'accorder l'accès aux documents requis par le demandeur.

18. Recommandation OFPER / Représentation linguistique des personnes occupant une fonction dirigeante dans l'administration fédérale (22 août 2013)

Le demandeur a déposé une demande d'accès auprès de l'Office fédéral du personnel (OFPER) et a requis l'accès à la répartition linguistique par langue maternelle des personnes occupant une fonction de directeur, membre de la direction ou de chef de division dans l'administration fédérale; ceci pour chaque office ou unité organisationnelle.

Le Préposé a constaté qu'au vu des informations transmises par l'OFPER, les fonctions de recherche automatique existantes ne permettent pas d'établir de façon automatisée le document requis.

Au vu de la complexité, de l'ampleur et de la durée des processus nécessaires à l'établissement de la statistique requise par le demandeur, le Préposé est arrivé à la conclusion qu'il ne saurait en l'espèce s'agir d'un traitement informatisé simple au sens de la LTrans.

19. Recommandation COMCO / Liste des collaborateurs (3 septembre 2013)

Le demandeur a requis entre autres l'accès à la liste des collaborateurs de la Commission de la concurrence (COMCO) qui ont travaillé sur les dossiers de rachat de Denner par Migros et de Fromalp par Emmi. La COMCO a refusé l'accès à ces documents en invoquant le fait que les dispositions de droit du travail du code des obligations (CO) interdisent le traitement et la divulgation des données en question.

Dans sa recommandation, le Préposé a conclu que ce n'est pas le Code des obligations, mais la loi sur le personnel de la Confédération (LPers) qui est déterminante quant à la publication des listes, la LPers n'étant toutefois pas une disposition spéciale au sens de la LTrans. Par ailleurs, le Préposé a estimé que permettre l'accès à ces données personnelles n'implique pas de répercussions défavorables pour les collaborateurs, et ne porte atteinte, si tel est le cas, que de manière minime à la sphère privée des personnes concernées et que, de ce fait, il n'y a pas d'obligation d'anonymisation. Ainsi, l'intérêt public à la transparence l'emporte sur l'intérêt à protéger la sphère privée de ces collaborateurs, raison pour laquelle l'accès à la liste avec les noms des collaborateurs doit être accordé, conformément à la recommandation du Préposé.

20. Recommandation OFAC / Examens de sécurité des décollages vers le sud sur une trajectoire rectiligne (16 straight) (4 septembre 2013)

Le demandeur a requis l'accès aux documents l'Office fédéral de l'aviation civile (OFAC) concernant les examens de sécurité à propos des pistes de décollage 10 et 34 de l'aéroport de Zurich. L'OFAC lui a refusé cet accès notamment au motif que ces documents concernent la procédure en cours «Plan sectoriel de l'infrastructure aéronautique» et sont exclus du champ d'application matériel de la LTrans en raison de cette procédure administrative de première instance. Par ailleurs, l'OFAC a estimé qu'une publication anticipée des documents demandés porterait considérablement atteinte à la libre formation de l'opinion et de la volonté du Conseil fédéral.

Dans sa recommandation, le Préposé a retenu que l'accès à une partie des documents demandés ne doit pas être accordé car ils ont été élaborés avant l'entrée en vigueur de la LTrans. De plus, il a conclu que l'accès ne doit pas non plus être accordé aux autres documents demandés – établis après l'entrée en vigueur de la LTrans – ceux-ci étant liés à un arrêté imminent du Conseil fédéral et concernant une procédure en cours.

21. Recommandation SG-DETEC / Données concernant des sociétés du groupe La Poste Suisse (11 septembre 2013)

Le demandeur a requis auprès du Secrétariat général du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (SG-DETEC) des renseignements concernant la vente et l'achat de sociétés étrangères du groupe La Poste Suisse ainsi que leurs comptes de profits et pertes. Le SG-DETEC lui a signalé les informations accessibles au public figurant dans le rapport d'activités de la Poste. Pour le reste, il a refusé l'accès requis, dans la mesure où les documents demandés étaient disponibles, en raison de l'existence de secrets d'affaires. Étant donné qu'au cours de la procédure de médiation, il est apparu que le Secrétariat

général du DETEC ne disposait effectivement pas des informations en question, le Préposé n'a pas tranché la question de savoir s'ils renfermaient des secrets d'affaires. En conséquence, il a donc suivi le refus partiel d'accès prononcé par le Secrétariat général du DETEC.

22. Recommandation OFAC / Suivi du trafic aérien de nuit à l'aéroport de Zurich (17 septembre 2013)

Le demandeur a requis auprès de l'Office fédéral de l'aviation civile (OFAC) l'accès aux résultats du suivi du trafic aérien de nuit à l'aéroport de Zurich, résultats établis par un groupe de travail. L'OFAC a remis au demandeur une documentation de sept pages comprenant des graphiques et des statistiques et l'a informé simultanément qu'il n'existait aucun autre document à ce sujet. Au cours de la procédure de médiation, il est apparu que le demandeur était essentiellement intéressé par les comptes-rendus de séance du groupe de suivi.

L'OFAC a refusé l'accès à ces documents au motif que l'échange d'informations au sein du groupe de travail était confidentiel et qu'une communication du contenu des séances mettrait en danger l'exécution de la pratique future en matière d'autorisation conformément aux objectifs fixés dans ce domaine par l'aéroport de Zurich, voire la rendrait totalement impossible.

Le Préposé a toutefois estimé qu'il n'y avait pas de garantie de confidentialité à propos du contenu des séances du groupe de suivi. En outre, il a considéré que l'OFAC n'avait pas présenté de manière juridiquement satisfaisante pour quelle raison et dans quelle mesure un accès à ces documents influeraient de manière négative sur la pratique future en matière d'autorisation dans le domaine du trafic de nuit à l'aéroport de Zurich. En définitive, il a recommandé à l'OFAC de permettre l'accès aux comptes-rendus de séance requis et à tous les autres documents officiels éventuellement disponibles concernant le suivi.

23. Recommandation SECO / Comptes-rendus des séances de direction et dossiers (18 septembre 2013)

Le demandeur a requis auprès du Secrétariat d'État à l'économie (SECO) l'accès aux procès-verbaux de séances de direction et aux fiches de travail, séries de transparents ou autres annexes pour la période allant d'août à décembre 2011. Le SECO a refusé cet accès en invoquant le fait que les comptes-rendus de séance ne sont pas des documents officiels. Et même s'ils l'étaient, l'office en refuserait l'accès. Il se fondait à cet égard sur diverses exceptions prévues par la Ltrans. Dans son avis adressé au Préposé, le SECO a réitéré ses arguments et précisé en outre que la demande d'accès concernait en tout 74 pièces.

Dans sa recommandation, le Préposé est parvenu à la conclusion que la prise de position transmise par le SECO au demandeur ne répondait pas aux exigences auxquelles doit répondre une motivation sommaire et n'a pas fourni une assistance suffisante au demandeur. À propos des comptes-rendus de séance, le Préposé a rappelé que ceux-ci constituent des documents officiels. Étant donné que le SECO avait fait valoir de manière globale pour l'ensemble des 74 pièces sur une brève page plusieurs exceptions au droit d'accès en vertu de la LTrans, il avait omis, de l'avis du Préposé, de renverser la présomption de libre accès pour chacun des documents. Par conséquent, le Préposé a recommandé l'accès à tous les documents en tenant dûment compte de la protection des données personnelles.

24. Recommandation ODM / Contrats d'objets - Centre de procédure - Domaine de l'asile (8 octobre 2013)

Le demandeur a requis l'accès à la convention de prestations entre l'Office fédéral des migrations (ODM) et la société ORS Service AG, ainsi qu'aux quatre derniers rapports d'activités que ce dernier avait transmis à l'ODM. Contrairement à l'ORS Service AG, l'ODM estimait que l'accès devrait être accordé aux contrats d'objets demandés. Au cours de l'audience de médiation qui a suivi, les parties ont établi dans une convention partielle que les conventions-cadres ne prévoyaient pas l'établissement de rapports d'activités, qu'il n'en existait pas et que les conventions-cadre ne faisaient pas l'objet de la procédure de médiation.

Au terme de l'audience de médiation, l'ORS Service AG a persisté dans son refus d'accorder l'accès aux contrats d'objets demandés au motif que le ratio d'encadrement y figurait et que l'indemnisation convenue constituaient des secrets professionnels qui devaient être noircis et rendus inaccessibles. En définitive, le Préposé a établi le 8 octobre 2013 une recommandation dans laquelle il concluait que les renseignements noircis ne constituaient pas des secrets professionnels et que l'accès aux contrats d'objets devait être accordé.

25. Recommandation OFAC / Données de radar concernant les vols (9 octobre 2013)

Le demandeur a déposé une demande auprès de l'Office fédéral de l'aviation civile (OFAC) et requis l'accès aux données de tous les vols (militaires) sans signal de transpondeur du 15 juin 2012. L'OFAC a renvoyé le demandeur à la société de contrôle de la navigation aérienne Skyguide parce qu'il n'était lui-même pas en possession des documents demandés. Skyguide a toutefois refusé l'accès au motif qu'elle n'entrait pas dans le champ d'application personnel de la LTrans.

Dans sa recommandation, le Préposé a conclu que c'était à juste titre que l'OFAC n'avait pas accordé l'accès à des documents dont il n'était pas en possession. En outre, il a établi que Skyguide accomplit incontestablement des tâches pour

le compte de la Confédération qui devraient normalement être assumées par l'administration centrale. Pour cette raison, le Préposé a assimilé Skyguide à l'administration fédérale et, de fait, l'a placé dans le champ d'application personnel de la LTrans.

26. Recommandation OFJ / Dossiers de procédure de la CEDH (10 octobre 2013)

Le demandeur a déposé auprès de l'Office fédéral de la justice (OFJ) une demande d'accès à un document que l'OFJ avait remis à la Cour européenne des droits de l'homme (CEDH) afin de demander le réexamen d'un jugement de la CEDH dans l'affaire «Gross c. la Suisse» auprès de la Grande Chambre.

L'OFJ a refusé l'accès à ce document au motif que la LTrans n'est pas applicable aux procédures devant la CEDH et que l'accès dans ce cas est régi séparément par le règlement de la CEDH.

Au regard des faits, le Préposé a constaté que le document élaboré par l'OFJ fait partie du dossier d'une procédure en cours devant la CEDH, procédure régie par un droit de procédure propre. Il a conclu que la disposition spéciale de l'article 33 du règlement de procédure de la CEDH est déterminante quant à l'accès au mémoire de l'OFJ. Le Préposé a soutenu le refus d'accorder l'accès prononcé par l'OFJ, au motif que le document requis est exclu, en tant que partie de la procédure judiciaire en cours, du champ d'application matériel de la LTrans et que de ce fait, la LTrans n'est pas applicable.

27. Recommandation OFEN / Sécurité sismique de la Centrale hydroélectrique de Mühleberg (15 octobre 2013)

Le demandeur a requis auprès de l'Office fédéral de l'énergie (OFEN) l'accès à des rapports et à un procès-verbal concernant le contrôle de la sécurité sismique de la Centrale hydroélectrique de Mühleberg. L'OFEN a refusé d'accorder au demandeur l'accès aux documents requis au motif que leur divulgation porterait atteinte à l'exécution, conforme aux objectifs visés, de la surveillance de la sécurité des barrages. Par ailleurs, l'office invoquait le fait que la confidentialité avait été garantie à tous les exploitants des barrages.

Dans sa recommandation, le Préposé a noté que l'activité de surveillance de l'OFEN peut être facilement poursuivie même après la publication des documents et que l'exécution, conforme aux objectifs fixés, de mesures concrètes émanant des autorités n'est pas compromise par la divulgation du procès-verbal demandé. Enfin, l'OFEN était dans l'incapacité de produire une garantie écrite de la confidentialité. S'agissant des données personnelles figurant dans les documents demandés, le Préposé a estimé que le nom des collaborateurs mentionnés membres de l'administration publique doivent être révélés et que les noms des autres personnes mentionnées dans le procès-verbal peuvent être anonymisés.

28. Recommandation ODM / Centre pour requérants d'asile du col du Jaun (29 octobre 2013)

Le demandeur a requis auprès de l'Office fédéral des migrations (ODM) l'accès à trois documents qui concernaient le Centre pour requérants d'asile du col du Jaun.

L'ODM lui a refusé cet accès au motif que la publication des documents en question entraverait les relations entre la Confédération et les cantons/communes ainsi qu'entre les cantons et les communes. L'ODM estimait en outre qu'il y aurait entrave aux mesures prises par les autorités dans le cadre des négociations concernant l'hébergement des requérants d'asile avec les cantons et les communes.

Au cours de la procédure de médiation, il est apparu que les documents que l'ODM a remis au Préposé n'étaient pas ceux que le demandeur désirait consulter. Il est ressorti que l'ODM ne disposait pas des documents demandés et que la prise de position remise ne se rapportait pas aux documents faisant l'objet du litige dans la procédure de médiation. Le Préposé étant tenu en définitive de se fier aux informations livrées par l'ODM et n'ayant en outre aucune raison de douter de la crédibilité de cet office, il s'est rallié à la décision de ce dernier de ne pas autoriser le demandeur à accéder aux documents requis.

Dans sa recommandation, le Préposé a relevé par ailleurs qu'il n'a lui-même aucune obligation de surveillance concernant la gestion des dossiers de l'administration fédérale.

29. Recommandation IFSN / Procès-verbaux de séances relatifs au contrôle de la sécurité sismique de la Centrale hydroélectrique de Mühleberg (30 octobre 2013)

Deux demandeurs ont requis auprès de l'Inspection fédérale de la sécurité nucléaire (IFSN) l'accès à des procès-verbaux de séances relatifs au contrôle de la sécurité sismique de la Centrale hydroélectrique de Mühleberg. L'IFSN en a refusé l'accès au motif qu'ils étaient en relation étroite avec une procédure cantonale d'octroi du permis de construire qui n'était pas encore close. Après avoir cependant constaté que la procédure devant le Tribunal administratif fédéral était close, le Préposé a enjoint l'IFSN de produire un nouvel avis.

L'IFSN a refusé la consultation des documents en invoquant une nouvelle fois une procédure en cours. Les recherches effectuées par le Préposé ont permis d'établir en définitive que les procès-verbaux de séances requis n'appartenaient pas au dossier de procédure cantonale. Pour cette raison, le Préposé a établi dans sa recommandation que l'accès doit être accordé aux documents demandés. En outre, le Préposé a estimé que l'IFSN n'avait pas présenté une motivation suffisante et conforme au droit ainsi que des éléments qui auraient justifié un refus.

30. Recommandation OFAC / Actes législatifs de la Commission européenne (19 novembre 2013)

Dans le cadre de la rédaction d'un mémoire, le demandeur a requis auprès de l'Office fédéral de l'aviation civile (OFAC) l'accès à des décisions non publiées de la Commission européenne concernant les mesures pour la mise en œuvre des normes de base communes de la sécurité aérienne.

L'OFAC a refusé l'accès aux actes normatifs en question au motif qu'il s'agit d'informations classifiées de l'UE auxquelles n'ont accès que les personnes qui en ont besoin pour l'exercice de leurs activités. L'office a ajouté que le demandeur ne fait pas partie de ce cercle de personnes car n'il exerce aucune tâche ou n'assume aucun mandat au service de l'aviation suisse et qu'en outre, la divulgation de ces décisions menacerait la sécurité intérieure et extérieure de la Suisse et serait une entrave aux relations internationales.

Le Préposé a conclu que le règlement sur la transparence de l'UE n'est applicable que lorsque la demande d'accès est présentée directement à la Commission européenne. En l'espèce, la demande d'accès a été adressée à l'OFAC de sorte que la LTrans est applicable car pour la Suisse, comme pour les États membres de l'UE, le droit national à l'accès aux documents officiels est le droit applicable. Il a estimé par ailleurs que les motifs d'exception visant la protection des intérêts publics conformément au droit de l'UE se trouvent aussi dans la LTrans.

Le Préposé s'est donc rallié au refus d'accès prononcé par l'OFAC car il a considéré comme démontré que la divulgation de ces décisions menacerait la sécurité intérieure et extérieure de la Suisse et compromettrait la sécurité internationale. Le Préposé a toutefois souligné que l'OFAC peut, s'il le veut, examiner la possibilité d'accorder en l'espèce au demandeur un accès conditionnel en raison de son intérêt prouvé à la recherche.

31. Recommandation OFEN / Règlement de surveillance du barrage du Wohlensee (28 novembre 2013)

Le demandeur a requis auprès de l'Office fédéral de l'énergie (OFEN) l'accès au règlement de surveillance du barrage du Wohlensee. L'OFEN a refusé cet accès au motif qu'il s'agissait d'un dossier de procédure et que la LTrans n'était pas applicable.

Dans sa recommandation, le Préposé est parvenu à la conclusion que le règlement de surveillance en question ne fait pas partie du dossier d'une procédure en cours, raison pour laquelle on ne peut différer son accès. Il a donc indiqué dans sa recommandation que l'accès au document demandé ainsi qu'à ses annexes doit être accordé.

32. Recommandation FNS / Documents en relation avec le Programme national de recherche «Fin de vie» (5 décembre 2013)

Le demandeur a requis auprès du Fonds national suisse (FNS) l'accès à plusieurs groupes de documents en relation avec le programme national de recherche mené par le FNS «Fin de vie» (PNR 67). Plus précisément, il a demandé que lui soient remis d'une part des documents relatifs à la préparation et à la proposition à l'intention du Conseil fédéral (requête A) et aux propositions de composition et de nomination du comité de direction du PNR 67 (requête B) et, d'autre part, des documents concernant neuf projets de recherche nommément cités, concernant les demandes de contribution en question (requête C), les noms des experts invités à se prononcer à ce propos (requête D) ainsi que les expertises elles-mêmes (requête E).

Suite à cette demande, le FNS a accordé l'accès aux documents concernant la requête A, mais avec anonymisation partielle des données personnelles qui y étaient contenues. Le FNS a rejeté les autres requêtes (B à E) sur la base de divers motifs.

Le Préposé a présenté les considérations suivantes dans sa recommandation: en premier lieu, les noms de personnes participant au PNR 67 qui ont été anonymisés doivent être communiqués par le FNS (requête A). De même, le FNS doit permettre l'accès aux propositions et aux décisions de nomination des membres du comité de direction du PNR 67 ainsi qu'aux extraits de procès-verbaux y relatifs (requête B), mais sans révéler le curriculum vitae détaillé des candidats. L'accès aux demandes de contributions concernant neufs projets de recherche nommément cités ne peut être accordé. Elles contiennent des informations sensibles sur les projets de recherche. Par contre, les simples formulaires d'inscription doivent être communiqués au demandeur (requête C).

Par ailleurs, le FNS ne peut divulguer les noms des experts œuvrant dans le cadre de la procédure d'évaluation par les pairs étant donné une disposition particulière figurant dans la loi sur l'encouragement de la recherche et de l'innovation (LERI) qui prévoit explicitement que les noms des experts ne peuvent pas être communiqués (requête D). En outre, l'accès aux expertises elles-mêmes ne peut être accordé au demandeur en raison du lien direct et étroit avec les demandes de recherche étant donné la nécessité de protéger les informations concernant les projets de recherche figurant dans ces demandes (requête E).

Enfin, le Préposé a estimé que la perception d'un émolument de 800 francs pour le traitement de cette demande d'accès est appropriée et de ce fait conforme à la loi.

33. Recommandation OFJ et SFI / Compétence pour le traitement d'une demande d'accès (18 décembre 2013)

Dans le cadre d'un projet de film documentaire sur le conflit fiscal entre les États-Unis et la Suisse, le demandeur a requis auprès de l'Office fédéral de la justice (OFJ) et du Secrétariat d'État aux questions financières internationales (SFI) l'accès à la correspondance échangée entre le directeur et le sous-directeur de l'OFJ ainsi qu'à la correspondance échangée entre ces derniers et la cheffe de département pour la période allant du 16 décembre 2011 au 18 janvier 2012.

Après s'être déclaré tout d'abord compétent pour le traitement de la demande d'accès et s'être en outre prononcé sur le fond, l'OFJ a convenu de la compétence du SFI dans le cadre de l'audition des offices concernés. Le SFI et l'OFJ ont justifié cette mesure par le fait que l'éventuelle livraison aux États-Unis des données concernant les collaborateurs n'était qu'un aspect partiel du dossier relatif au conflit fiscal avec les États-Unis dont le SFI avait la direction. Les deux organes argumentaient en outre que les documents de la FINMA n'étaient pas accessibles en vertu de la LTrans car elle n'était pas soumise à cette loi.

Le Préposé a conclu que les documents de la FINMA envoyés à une autorité soumise à la LTrans sont accessibles sous réserve des exceptions légales. En premier lieu, le Préposé a examiné la question de savoir si la compétence convenue par l'OFJ et le SFI est conforme à la loi. Il a tout d'abord relevé que les prescriptions de coordination figurant dans l'ordonnance servent uniquement à faciliter l'accès à la personne qui le demande. Ayant considéré comme non rempli le critère de «la même affaire» au sens de l'article 11, al. 2, OTrans, il a concrètement rejeté la compétence du SFI. De même, il a considéré que concentrer le traitement de l'accès auprès d'une autorité n'est pas compatible avec le concept de la LTrans.

Enfin, le Préposé a expliqué que l'OFJ est l'autorité compétente pour le traitement de la demande d'accès pour les documents qu'il a établis lui-même, ainsi que pour les documents qu'il a reçus de tiers, y compris de la FINMA. Étant donné que l'OFJ n'avait pas livré d'avis définitif sur la demande d'accès, le Préposé ne s'est pas prononcé sur les motifs d'exception sur le fond avancés par l'OFJ et le SFI.

34. Recommandation OFCL / Documents concernant l'évaluation et la statistique du controlling des achats 2011 pour tous les départements et la Chancellerie fédérale (23 décembre 2013)

Les demandeurs ont requis auprès de l'Office fédéral des constructions et de la logistique (OFCL) l'accès aux rapports de controlling ainsi qu'à l'analyse des statistiques concernant les chiffres des marchés publics 2011 des départements et de la Chancellerie fédérale (ChF). Mis à part quelques documents que l'OFCL a rendus accessibles sans restriction, les demandeurs ont été autorisés à consulter

huit tableaux contenant la liste des 40 principaux créanciers (fournisseurs) des départements et de la ChF. Invoquant la protection des secrets d'affaires, l'OFCL avait anonymisé les noms de ces 40 entreprises. L'office soutenait en effet qu'un accès à ces listes n'entrait pas en ligne de compte sans anonymisation car une combinaison des informations ainsi livrées, y compris les noms des entreprises, constituerait un secret commercial digne d'être protégé et dont la divulgation mènerait à une distorsion de concurrence.

S'adressant au Préposé, l'OFCL a en outre invoqué dans le cadre de sa restriction d'accès une note de discussion du Conseil fédéral du 23 avril 2013, rédigée dans le contexte de la demande d'accès à examiner, ainsi qu'un arrêté y relatif du Conseil fédéral daté du 1er mai 2013 selon lequel une anonymisation des noms des entreprises figurant dans la liste est prévue de manière impérative (voir également chiffre 2.5.2 du présent rapport d'activités).

Dans sa recommandation, le Préposé a conclu que les noms jusqu'ici anonymisés des 40 plus gros fournisseurs des départements et de la ChF doivent être entièrement rendus publics. Pour les acquisitions atteignant les valeurs de seuil du droit des marchés publics, la publication des entreprises retenues est même prescrite par la loi et, de ce fait, une disposition spéciale du droit des marchés publics est applicable. Pour ce qui est des acquisitions inférieures aux valeurs de seuil, le Préposé a écarté la présence d'une disposition d'exception. Il considère en particulier qu'il n'est pas admissible d'invoquer la protection des secrets d'affaires.

En outre, le Préposé a estimé que les trois propositions de solution de la note de discussion mentionnée et de l'arrêté y relatif du Conseil fédéral du 1er mai 2013 ne sont pas compatibles en l'espèce avec les dispositions de la LTrans et les a par conséquent rejetées. Enfin, il a conclu que tous les autres documents officiels éventuellement existants dans ce contexte devaient être rendus accessibles conformément aux prescriptions de la LTrans.

35. Recommandation Swissmedic / Décision d'émolument (23 décembre 2013)

Le demandeur a requis auprès de Swissmedic l'accès à une liste de tous les documents en relation avec l'homologation du Tamiflu. Après avoir précisé sa demande d'accès et reçu tous les documents requis, il a alors contesté dans une demande en médiation uniquement le prélèvement des émoluments.

Dans sa recommandation, le Préposé a précisé qu'il fallait prendre en compte les efforts de précision du demandeur pendant la procédure d'accès et a renvoyé le demandeur à Swissmedic afin qu'il rende une nouvelle décision sur l'émolument.

2.3.2 Médiations

Ci-après une sélection de cas dans lesquels une solution consensuelle a été trouvée durant l'année sous revue.

1. Médiation DDPS / Conseil consultatif pour le développement de l'armée

Le demandeur avait requis auprès du DDPS l'accès à des documents concernant un éventuel paiement et dédommagement du Conseil consultatif pour le développement de l'armée, ainsi que d'autres documents établis depuis la création dudit conseil. Après examen des documents en question par le Préposé à l'occasion d'une réunion avec le DDPS, le département s'est déclaré prêt à remettre au demandeur tous les documents requis. Un règlement amiable a ainsi été trouvé.

2. Médiation DETEC / Vœux de Noël et de Nouvel An

Le demandeur avait requis auprès du DETEC la «liste des chefs d'États, organisations et offices ainsi que des autres personnes qui ont reçu en 2010 des vœux de Noël et de Nouvel An de la part de la Présidente de la Confédération Doris Leuthard». En réponse à notre demande, il a expressément renoncé aux adresses de particuliers.

Au cours de la procédure de médiation, le Préposé est parvenu à la conclusion que la LTrans ne prévoyait pas de disposition d'exception qui justifierait de refuser ou de différer la révélation de la liste en question. Le DETEC a pris connaissance de l'avis du Préposé et s'est déclaré prêt à remettre au demandeur une liste des personnes remplissant une fonction politique. Le demandeur a accepté cette liste.

3. Médiation IFSN / Chemin d'accès concernant des décisions

Le demandeur avait requis auprès de l'IFSN l'accès aux originaux des décisions que l'IFSN avait mis en ligne sur Internet. Grâce à la médiation du Préposé, les parties ont trouvé un accord, à savoir: l'IFSN a été en mesure de présenter de manière claire au demandeur les démarches qui avaient mené aux différents chemins d'accès des décisions publiées et le demandeur a considéré sa requête comme réglée.

4. Médiation OFAG / Précision de la demande d'accès

Le demandeur avait requis auprès de l'OFAG l'accès aux listes des destinataires des suppléments versés pour le lait transformé en fromage, ceux-ci étant basés sur le soutien du prix du lait pour la période allant de 2006 à 2011. Il demandait également pour la même période la liste des destinataires des suppléments versés pour le non-ensilage.

Le demandeur et l'OFAG avaient convenu de limiter la demande d'accès aux 40 principaux bénéficiaires des suppléments pour le lait transformé en fromage et

pour le non-ensilage de 2006 à 2011, ainsi que de l'étendre dans la même mesure à l'année 2012. Aucun accord n'ayant pu être obtenu, le Préposé a émis une recommandation le 7 août 2013 (voir chiffre 2.3.1 du présent rapport d'activités, recommandation n°16).

5. Médiation OFEN / Procès-verbaux de séances de la CSN

Le demandeur avait requis auprès de l'OFEN l'accès à tous les procès-verbaux de séances de la Commission fédérale pour la sécurité nucléaire (CSN) pour l'année 2011. Après réception et consultation de la recommandation du Préposé du 16 décembre 2011, l'OFEN a réexaminé les documents requis par le demandeur et a conclu qu'il était possible d'en accorder un accès presque complet. Au terme d'échanges écrits et téléphoniques entre le requérant, le Préposé et l'OFEN, l'office a soumis au demandeur une proposition d'accord que ce dernier a acceptée.

6. Médiation ODM / Contrats d'objets concernant les centres de procédure dans le domaine de l'asile

Le demandeur avait requis l'accès à la convention de prestations actuelle de l'ODM avec la société ORS Service AG, ainsi qu'aux quatre derniers rapports d'activités que l'ORS Service AG avait transmis à l'ODM. Au cours de l'audience de médiation, les parties ont établi dans une convention partielle que les conventions-cadres ne prévoyaient pas l'établissement de rapports d'activités, que de tels rapports n'existaient pas et que les conventions-cadres ne faisaient pas l'objet de la procédure de médiation. Concernant les points en suspens, le Préposé a établi le 8 octobre 2013 une recommandation et conclu que les passages noircis ne constituaient pas des secrets professionnels et que l'accès aux contrats d'objet devait par conséquent être accordé (voir chiffre 2.3.1 du présent rapport d'activités, recommandation n°24)

7. Médiation DFAE / Coopération au développement

Le demandeur avait requis l'accès aux rapports de suivi, rapports annuels et rapports d'évaluation des années 2007 à 2010 de Swisscontact et de la DDC concernant trois projets de développement (Népal, Kenya et Bolivie). Par ailleurs, il désirait consulter la liste de tous les mandats qui avaient été accordés en 2011 aux organisations Helvetas, Intercooperation, Helvetas Swiss Intercooperation et Swisscontact.

Au cours de la procédure de médiation, le demandeur a trouvé un accord avec le DFAE concernant les rapports relatifs à un projet (Kenya) et a retiré sa requête sur ce point. Faute d'accord sur les autres documents livrés et surtout sur les deux factures d'émoluments d'un montant total de 1300 francs, une audience de médiation a été tenue le 25 octobre 2013. Dans ce cadre, les parties ont convenu d'un accès à l'ensemble des documents concernant les deux autres projets (Népal

et Bolivie) dans la mesure où l'accès n'avait pas été déjà accordé par le DFAE. Les émoluments dus pour ces deux demandes partielles ont été renégociés. Au terme de cette procédure, le DFAE a également fini par accorder au demandeur l'accès à une liste complète des mandats attribués aux quatre organisations citées pendant l'année 2011.

8. Médiation OFS / Statistique du tourisme

Le demandeur avait requis l'accès à plusieurs documents sur la statistique du tourisme. Au terme d'un entretien avec l'OFS, le Préposé a invité les parties à une procédure de médiation. Elles ont convenu que l'office remette au demandeur dans le délai imparti un document précis avec les caviardages effectués par l'OFS. Par ailleurs, l'OFS s'est déclaré prêt dans la convention de médiation à mener avec le demandeur un entretien personnel concernant son projet de recherche.

9. Médiation OFAS / Rapports d'audit Office AI et SMR Zurich

Le demandeur a requis l'accès aux deux derniers rapports d'audit concernant l'office AI et le Service de médecins régionaux (SMR) Zurich de l'OFAS. Dans le cadre de la procédure de médiation, divers entretiens ont eu lieu entre le Préposé et le demandeur d'une part et le Préposé et l'OFS d'autre part. Suite à ces discussions, les documents en question ont été présentés pour consultation au demandeur avec un petit nombre de passages anonymisés. Enfin, dans une convention, les parties ont déclaré avoir réglé le conflit et ont demandé ensemble la clôture de la procédure de médiation.

2.4 Décisions judiciaires relatives à la loi sur la transparence

2.4.1 Tribunal administratif fédéral

Ci-après une sélection de jugements que le Tribunal administratif fédéral (TAF) a prononcés en 2013 en rapport avec l'octroi d'un accès aux documents officiels:

1. OFAS / Procès-verbaux des séances de la Commission de l'AVS/AI

L'Office fédéral des assurances sociales (OFAS) a rendu une décision en contradiction avec la recommandation du Préposé du 16 août 2012 (cf. notre rapport d'activités 2012/2013, ch. 2.3.1), et qui a été portée devant le TAF. Le recourant a demandé l'annulation de la décision et l'octroi d'un accès aux procès-verbaux des séances de la Commission de l'AVS/AI. Il a fait valoir que la Commission faisait partie, depuis l'entrée en vigueur des amendements à la loi sur l'organisation du gouvernement et de l'administration (LOGA), de l'administration fédérale décentralisée et était de ce fait soumise à la loi sur la transparence. L'OFAS a en revanche fait valoir que la Commission de l'AVS/AI devait être considérée comme une commission administrative et n'était donc pas soumise à la loi sur la transparence. L'OFAS a motivé cette appréciation en invoquant la volonté du législateur.

Quant à la question de savoir si les commissions administratives relèvent de la loi sur la transparence, le tribunal a examiné à fond l'interprétation de la LTrans et de la LOGA. Il est arrivé à la conclusion que toutes les méthodes d'interprétation mènent au même résultat, à savoir que les commissions instituées par les autorités ainsi que les commissions administratives font toutes deux partie de l'administration fédérale décentralisée et sont ainsi soumises à la loi sur la transparence. Les commissions de l'AVS/AI ne seraient exclues que s'il existait une dérogation explicitement prévue par le Conseil fédéral. Le tribunal a admis le recours et annulé la décision. Il a octroyé l'accès aux procès-verbaux demandés en l'espèce, étant donné que l'OFAS ne s'était pas exprimé sur des motifs d'exception, ni dans sa décision, ni dans sa prise de position, et avait omis de réfuter la présomption de libre accès.

En ce qui concerne la protection des données personnelles, le tribunal a déclaré que l'OFAS avait également omis de s'exprimer sur ce point. Il a ordonné à l'Office d'anonymiser par noircissement les noms des personnes physiques, à l'exception de ceux des collaborateurs des autorités et des membres de la Commission ainsi que les noms des représentants des institutions et organisations, pour autant que ceux-ci n'exercent pas une fonction officielle (jugement du 22 avril 2013, réf.A-4962/2012).

2. ESTI / Liste des appareils électriques contrôlés

Le rédacteur en chef du magazine des consommateurs saldo avait demandé à l'Inspection fédérale des installations à courant fort (ESTI) d'accéder à la liste des appareils électriques qui avaient été contrôlés en 2011, incluant les résultats des contrôles et les interdictions de vente prononcées. L'ESTI a finalement fourni les documents au requérant en lui imposant un émolument de 700 francs. Le requérant a recouru contre cette décision devant le TAF, demandant l'annulation de la décision fixant les émoluments et l'octroi d'un accès exempt de frais.

Le TAF s'était déjà exprimé dans le passé sur l'admissibilité d'une perception d'émoluments auprès des correspondants des médias pour l'accès aux documents officiels (cf. le jugement déjà référencé du TAF 1200/2012 du 27 novembre 2012 dans notre rapport d'activités 2012/2013, ch. 2.4.1).

Dans son arrêt, le TAF a réaffirmé que les correspondants des médias n'avaient aucun droit constitutionnel à un accès exempt de frais aux documents officiels. Il a précisé que le Conseil fédéral n'avait d'ailleurs pas prévu un tel privilège dans l'ordonnance sur la transparence. Le TAF a par conséquent considéré comme admissible de percevoir un émolument également pour les correspondants des médias. Le tribunal a donc considéré qu'une exemption d'émoluments pour les correspondants des médias n'était indiquée que dans les cas où ceci concerne des services qui sont d'une importance vitale pour l'État ou la personne concernée, ce qui selon les juges n'était pas le cas dans l'affaire jugée.

En conséquence, le TAF a considéré la perception de frais auprès du journaliste comme étant en principe licite. Il a néanmoins réduit le montant dû de 100 francs, les dispositions de la LTrans ne permettant pas de demander un émolument pour l'établissement d'une décision (arrêt du 22 avril 2013, réf. A-3363/2012).

3. SECO / Documents d'un syndicat concernant une Convention collective

Dans un autre cas, le SECO a, sur la base de notre recommandation du 18 septembre 2012, rendu une décision qui a été portée devant le TAF. Dans ce cas, le recourant avait à l'origine demandé au SECO de lui donner accès à des documents présentés par des syndicats, qui demandaient que certaines dispositions de la Convention Collective pour la retraite anticipée dans le second œuvre romand (CCRA), notamment concernant la preuve des quorums existants, soient déclarées de force obligatoire générale.

Le SECO a refusé l'accès, en invoquant qu'il existait un lien direct et immédiat entre les documents demandés et la décision imminente du Conseil fédéral en la matière. Étant donné que le Conseil fédéral avait, dans le cadre de la procédure

de recours devant le Tribunal administratif fédéral concernant la modification de certaines dispositions de la déclaration de force obligatoire générale de la CCRA, pris une décision et qu'il n'y avait pas de dispositions d'exception de la LTrans, le TAF a accepté le recours dans son jugement du 8 octobre 2013 et a ordonné au SECO d'accorder au recourant l'accès aux documents présentés. (Arrêt du 8 octobre 2013, réf. A-5489/2012).

4. SECO / Décomptes de commissions paritaires I

Dans un autre arrêt, le TAF a examiné le recours déposé par plusieurs commissions paritaires contre une décision prise par le SECO, conformément à la recommandation du Préposé du 20 février 2013 (voir chiffre 2.3.1 du présent rapport d'activités, recommandation n°3. L'objet du recours était l'accès à des décomptes de l'an 2010, que les commissions paritaires devaient remettre à l'autorité de surveillance SECO. Les recourantes critiquaient entre autres la violation du droit d'être entendu, faisant valoir que les décisions du SECO s'appuyaient uniquement sur les considérants contenus dans la recommandation du Préposé.

Le tribunal a retenu que le SECO était autorisé à renoncer exceptionnellement à une justification détaillée, étant donné qu'il était d'accord sur tous les points avec la recommandation du Préposé et que les recourantes n'avaient pas motivé leurs demandes de rendre une décision dans la procédure de première instance. Contrairement à l'opinion des recourantes, le tribunal a déclaré que la LTrans était applicable aux décomptes des commissions paritaires organisées selon le droit privé. Il a explicitement retenu que le champ d'application de la LTrans devait être interprété de manière large, notamment en ce qui concerne les informations en provenance de sources privées et que ces informations devaient en principe être accessibles, dans la mesure où elles pouvaient être qualifiées de documents officiels.

Le tribunal a également déclaré, d'une part, que la personne déposant une demande d'accès à des documents privés, qui permettent une activité de surveillance, n'était pas tenue de démontrer un intérêt particulier, d'autre part que la LTransne prescrivait pas une finalité particulière. Dans la mesure où l'intimée devait, si l'accès lui est autorisé, constater des irrégularités dans les décomptes et en faire part, ceci permettrait en même temps de porter un regard sur l'activité de surveillance du SECO. Un abus de droit ne doit pas être accepté à la légère, étant donné qu'une demande d'accès symbolise la transparence de l'administration et que l'intimée fait usage de droits qui lui sont conférés par la LTrans.

Sur le fond, le tribunal a nié l'existence de motifs exceptionnels, mis à part la protection de certaines données personnelles. Il a fait remarquer que le noircissement des numéros de comptes bancaires et postaux aurait, dans un souci de clarté, dû être

inclus dans la décision et que les données personnelles des tierces personnes non impliquées dans la procédure devaient être noircies. Le tribunal a cependant réfuté une anonymisation plus poussée telle que demandée par les recourantes et a déclaré que le public avait un intérêt important à pouvoir reconstituer l'activité de surveillance d'une autorité, ce qui impliquait l'octroi d'un accès aux décomptes.

Finalement, le tribunal s'est exprimé sur le changement de pratique du SECO. Avant tout, le tribunal s'est demandé si une pratique usuelle s'était établie pour les demandes d'accès aux décomptes des commissions paritaires. Il en est venu à la conclusion que l'intérêt à une application correcte de la loi devait être jugé plus important que l'intérêt individuel des recourants. Le SECO aurait pu renoncer à annoncer un éventuel changement dans la pratique. La procédure de conciliation devant le Préposé serait d'ailleurs privée de son sens si les autorités n'avaient pas par la suite, grâce à une meilleure compréhension de la «ratio legis» et sur la base des recommandations du Préposé, la possibilité de dévier de l'opinion qu'ils avaient initialement défendue (arrêt du 9 décembre 2013, réf. A-2434/2013). En ce qui concerne les frais que doit supporter la partie qui n'a pas participé à la procédure de recours, se reporter au jugement suivant.

5. SECO / Décomptes de commissions paritaires II

Le TAF a examiné une autre décision rendue par le SECO, suite à la recommandation du Préposé du 20 février 2013 (cf. chiffre 2.3.1 de notre présent rapport d'activités, recommandation n°3. Cette décision est liée au jugement précité, qui avait pour objet l'accès aux décomptes de plusieurs commissions paritaires pour l'année 2010.

La recourante (une commission paritaire) a critiqué que le SECO n'avait manifestement pas réalisé que le Préposé avait, dans son cas, recommandé de rejeter la demande d'accès et que le dispositif de la décision était en contradiction avec les considérants du Préposé. La recourante a en outre fait valoir que la LTrans n'était pas applicable aux commissions paritaires organisées selon le droit privé.

Le SEC était d'avis que la recourante n'avait aucun intérêt digne de protection à obtenir l'accès. Conformément à la recommandation du Préposé, l'accès aux décomptes n'avait pas été accordé parce que la recourante n'était pas tenue d'en fournir pour l'année 2010.

Le tribunal a admis le recours. Il a annulé la décision en invoquant un vice de forme de l'instance antérieure et a également constaté qu'il n'existait pas de document officiel. Quant aux autres griefs de la recourante, le tribunal ne les a pas considérés. En ce qui concerne les frais, le tribunal a retenu qu'une partie qui a déposé des demandes dans la procédure de première instance ou a lancé la procédure ne

peut pas se soustraire à son obligation de supporter les frais dans une procédure de recours intentée par une autre partie. Elle continue à être la partie adverse nécessaire et doit donc supporter les frais, dans la mesure où elle n'a pas obtenu gain de cause en première instance.

Des exceptions ne sont justifiées que si le recours est admis suite à un vice de procédure qui ne lui incombe pas et que l'intimée a demandé l'admission du recours ou n'a pas déposé de demande. Dans le cas d'espèce, les parties ont exceptionnellement été exonérées des frais de procédure, étant donné que les raisons ayant conduit à l'admission du recours sont des vices de procédure imputables à l'instance antérieure, le SECO (arrêt du 9 décembre 2013, réf. A-2064/2013).

2.4.2 Tribunal fédéral

Le rédacteur en chef du magazine des consommateurs saldo a déposé un recours contre l'arrêt du TAF mentionné ci-dessus, demandant d'annuler ce jugement TAF et de le dispenser, en sa qualité de journaliste, du paiement d'émoluments pour l'accès à la liste demandée.

Dans son arrêt, le Tribunal fédéral a reconnu, contrairement à l'instance précédente, qu'il existait un intérêt public à accéder à des documents officiels qui pouvait justifier une exonération d'émoluments. Il a toutefois également relevé que l'autorité disposait d'un certain pouvoir d'appréciation qui lui permet de prendre en compte non seulement le coût occasionné par l'accès à l'information, mais aussi l'intérêt public de l'accès aux documents officiels.

En tenant dûment compte des circonstances spécifiques du cas évalué, le Tribunal fédéral est arrivé à la conclusion que l'ESTI n'aurait pas dû comptabiliser six heures de travail et facturer un émolument de 600 francs. Il s'est prononcé en faveur d'une réduction de l'émolument de 50 pour cent au moins, tout en laissant à l'ESTI le soin de décider s'il voulait réduire l'émolument ou y renoncer complètement, conformément à son pouvoir d'appréciation de ce dernier; il lui a donc renvoyé l'affaire (arrêt du 19 novembre 2013, réf. 1C_550/2013). Avec ce jugement, le Tribunal fédéral confirme la jurisprudence relative à la perception d'émoluments auprès des journalistes pour l'accès aux documents officiels introduite avec l'ATF 139 I 114, dans lequel il avait annulé le jugement du TAF.

2.5 Consultation des offices et autres prises de position

2.5.1 Projet de proposition au Conseil fédéral relative au message concernant la loi sur le renseignement

Dans le cadre de la consultation des offices, le Préposé a une nouvelle fois pris position sur le projet de proposition au Conseil fédéral relative au message concernant la loi sur le renseignement (cf. notre rapport d'activités 2012/2013, ch. 2.5.4).

Il a encore une fois relevé que l'exclusion de la «collecte d'informations selon la loi sur le renseignement» du champ d'application matériel était aussi bien en contradiction avec la finalité qu'avec la systématique de la loi sur la transparence. De plus, le projet ne prévoit pas de différencier les informations du Service de renseignement (SRC) en fonction de leur niveau de sensibilité.

Le Préposé a souligné que les instruments de la loi sur la transparence, avec toutes ses dispositions d'exception, suffisaient amplement pour répondre au besoin de protection accru du SRC. Enfin, il a une nouvelle fois relevé qu'il était éminemment important, au vu du sens et de la finalité de la loi sur la transparence, de concéder à la population un minimum de transparence administrative, surtout dans les domaines sensibles du pouvoir public. Cela a d'ailleurs été démontré par les récents événements en relation avec l'agence de renseignement américaine NSA.

Enfin, se basant sur la statistique annuelle des demandes d'accès selon la LTrans reçues par l'administration fédérale au cours de l'année, le Préposé rappelle que le faible nombre de douze demandes d'accès auprès du SRC soulève déjà la question de savoir si une exclusion du champ d'application de la LTrans peut être justifiée. Si l'on considère que sur ces douze demandes, un accès limité ou retardé a été accordé dans trois des cas et un accès sans restriction dans un des cas, la nécessité d'un statut spécial pour le SRC devient encore moins évidente.

La position du Préposé rejoint l'exigence de la Conférence internationale des commissaires à l'information, qui demande dans sa Déclaration de Berlin que le principe de la transparence soit également applicable aux services de renseignement (voir chiffre 2.7.1 du présent rapport d'activités).

2.5.2 Projet de document de travail du Conseil fédéral relatif au contrôle des achats dans l'administration fédérale

Dans le cadre de la consultation des offices sur le projet de document de travail du Conseil fédéral concernant l'accès aux documents officiels en vertu de la loi sur la transparence, le Préposé a pris position sur le contrôle des achats dans l'administration fédérale («Loi sur la transparence: accès à des documents officiels concernant le controlling des achats de l'administration fédérale; résultats de la Conférence des Secrétaires généraux du 17 décembre 2012»). Le projet prévoyait entre autres que les documents officiels, qui répertorient les noms de créanciers (fournisseurs) d'un organe fédéral triés selon le chiffre d'affaires réalisé et qui contiennent également des données permettant d'identifier les entreprises concernées, doivent être anonymisés par l'autorité responsable avant d'être rendus accessibles. En outre, le projet prévoyait également des règles divergentes en ce qui concerne les compétences pour le traitement des demandes d'accès selon la loi sur la transparence.

Le Préposé a exprimé son désaccord avec la position du document de travail selon laquelle une liste des 40 fournisseurs avec le plus grand chiffre d'affaires, accompagnée d'une description sommaire des prestations et du montant, constituerait une information qui, au vu du catalogue des exceptions de la loi sur la transparence, doit être protégée comme secret commercial. Il est au contraire d'avis que le droit des marchés publics prévoit explicitement la publication de ces informations.

Ensuite, le Préposé a relevé qu'il existait un intérêt public prépondérant à la publication des noms des entreprises impliquées, un aspect que le projet de document de travail ne prend pas du tout en compte. Ainsi, la LTrans demande explicitement que l'accès aux documents officiels contenant des données personnelles puisse être accordé, malgré une éventuelle atteinte à la sphère privée des personnes concernées, dans les cas où l'intérêt public à l'accès est prépondérant. C'est d'ailleurs précisément dans les cas de relations particulières entre autorités et personnes privées que l'ordonnance sur la transparence admet un intérêt public prépondérant, pour autant que cette relation procure des avantages significatifs à la personne privée. Elle argumente qu'il s'agit finalement de rendre des comptes au contribuable sur l'utilisation de millions d'impôts.

En ce qui concerne les compétences pour le traitement des demandes d'accès, le Préposé a fait remarquer que cette question était réglée dans la loi sur la transparence, qui prend uniquement en compte l'autorité qui a créé le document demandé ou l'a reçu comme destinataire principal.

En ce qui concerne les solutions proposées par le document de travail et la décision correspondante du Conseil fédéral du 1er mai 2013, le Préposé a par ailleurs pris position de façon détaillée dans sa recommandation du 23 décembre 2013 à l'Office fédéral des constructions et de la logistique (OFCL) (cf. notre rapport d'activités 2013/2014, ch.2.3.1, recommandation n°34).

2.6 Varia

2.6.1 Participation au groupe de travail «Lignes directrices concernant la perception d'émoluments LTrans»

Dans le cadre de la discussion sur le traitement des demandes LTrans déposées par des journalistes, la Conférence des secrétaires généraux (CSG) a mandaté le groupe «Protection des données» d'élaborer, en collaboration avec le Préposé et l'OFJ, des directives pour la perception d'émoluments sur les demandes d'accès. Le Préposé a participé comme expert dans un groupe de travail institué par le groupe «Protection des données» et dirigé par la Chancellerie fédérale. Il a ainsi apporté son point de vue et soumis plusieurs propositions concernant la perception d'émoluments.

Toutefois, le groupe de travail n'a que partiellement tenu compte de ces propositions dans le projet soumis au groupe «Protection des données». Il y a plusieurs divergences par rapport au projet: ainsi, le Préposé est d'avis que les directives doivent être conformes à l'article 17, al.1 LTrans. Si le législateur avait effectivement voulu une obligation absolue de payer des émoluments, il n'aurait pas ajouté la précision «en principe» dans cette disposition. Par conséquent, le Préposé considère cette formulation comme un droit de percevoir des émoluments. Si les dispositions d'exécution limitent le pouvoir d'appréciation des autorités, ceci constitue une violation du principe de la légalité.

En outre, le Préposé est d'avis que le législateur a délibérément renoncé à régler la question des frais d'expédition. Cet avis est d'ailleurs appuyé par les explications de l'OFJ datant de 2005 concernant les aspects organisationnels et techniques de l'application du principe de transparence. En outre, le Préposé est d'avis que la combinaison de deux intérêts (l'intérêt public à un accès aux documents officiels et l'intérêt public à un accès exempt de frais) peut créer la confusion et n'est pas réalisable en pratique. Finalement, il s'oppose au régime d'émoluments proposé pour les journalistes. D'une part, une réduction des émoluments limitée à 20 pour cent restreint la marge de manœuvre de l'autorité de sorte qu'une réduction plus conséquente ou un renoncement à l'émolument n'est plus possible. D'autre part, la réglementation prévue n'est conforme ni au concept de la loi sur la transparence, ni à l'arrêt du tribunal fédéral (cf. ATF 139 I 114).

Le groupe «Protection des données» a pris connaissance du projet du groupe de travail et l'a ensuite transmis à la CSG. Celle-ci a débattu des recommandations du groupe «Protection des données» pour ensuite les adopter formellement lors de sa séance du 22 novembre 2013. En contradiction avec le projet du groupe de travail, la CSG a inclus une réglementation spéciale pour les journalistes, qui prévoit que l'émolument pour leurs demandes peut être réduit de 20 pour cent.

Bien que le Préposé estime qu'il n'existe pas de droit à pouvoir accéder gratuitement aux documents officiels, il continue à défendre l'avis qu'il est indiqué – dans le cadre du pouvoir d'appréciation prévu à l'article 17, al.1 LTrans – de renoncer à percevoir un émolument, aussi pour les journalistes. Cette position correspond également à la jurisprudence la plus récente du Tribunal fédéral qui a précisément examiné la perception d'émoluments pour les journalistes. Le tribunal a nié le droit à être dispensé de l'émolument, mais a toutefois jugé que ce dernier devait être réduit de moitié au moins. Il a donc, en d'autres termes, confirmé qu'une réduction de plus de 50 pour cent dans des cas individuels était possible (arrêt du Tribunal fédéral 1C_550/2013 du 19 novembre 2013, voir notre rapport d'activités 2013/2014, ch. 2.4.2).

2.6.2 Congrès sur le principe de la transparence

En collaboration avec l'Office fédéral de la justice (OFJ), le Préposé a organisé le 24 février 2013 la deuxième «Journée de la transparence» à l'intention des conseillers et des conseillères à la transparence de l'administration fédérale. Cette rencontre a permis d'une part aux autorités chargées de l'application des lois d'échanger leurs expériences, d'autre part au Préposé, à l'OFJ et à la ChF de fournir des réponses aux questions souvent posées concernant la loi sur la transparence.

Suite à cette rencontre, le Préposé et l'OFJ ont révisé le document «Mise en œuvre du principe de transparence dans l'administration fédérale: questions fréquemment posées», qui datait de 2010. Le document contient maintenant, en plus des questions et réponses précédemment incluses, les questions qui ont été traitées lors de cette rencontre. Le document «FAQ sur la mise en œuvre du principe de la transparence» est disponible sur notre site web www.leprepose.ch, dans la rubrique Principe de la transparence – Documentation.

2.6.3 Relations avec les offices de conciliation cantonaux – groupe de travail sur la médiation

Le Préposé ainsi que les conseillers cantonaux à la transparence, qui mènent également des procédures de conciliation, se sont à nouveau rencontrés en 2013 pour un échange d'expériences. Ceci a permis, dans le cadre du «Groupe d'intervision sur la gestion consensuelle des conflits en matière de transparence» mis sur pied en automne 2011, de débattre des questions relatives à l'activité de médiation et au principe de la transparence. Cette collaboration est particulièrement importante et précieuse pour les acteurs impliqués, étant donné que la législation sur la transparence est un domaine du droit encore récent et que les expériences pratiques, la jurisprudence et la doctrine sont encore assez rares.

2.7 Conférence internationale des commissaires à l'information

Des commissaires à l'information du monde entier demandent dans une résolution de renforcer le droit d'accéder aux informations et d'améliorer la transparence de l'action gouvernementale.

La huitième Conférence internationale des commissaires à l'information s'est tenue du 18 au 20 septembre 2013 à Berlin. Elle a réuni des délégués en provenance de 35 États. La partie publique de la conférence a abordé des questions d'actualité touchant à la transparence de l'action gouvernementale. Les principaux thèmes ont été «La transparence au sein des controverses» et «Les médias et la politique Internet».

Dans la partie interne, lors de leur conférence de clôture, les commissaires à l'information ont adopté la «Déclaration de Berlin pour renforcer la transparence au niveau national et international». Dans cette résolution, ils exigent, sous le titre «Transparence - le carburant de la démocratie», de renforcer le droit d'accès à l'information et d'étendre l'obligation de transparence de l'action gouvernementale. La «Déclaration de Berlin» stipule en outre que les services secrets ne peuvent pas par principe refuser la transparence. Du fait justement que leurs activités peuvent porter gravement atteinte aux droits fondamentaux des citoyens et citoyennes, un contrôle constitutionnel est absolument nécessaire.

Les commissaires à l'information optent en faveur de la création, aussi bien au niveau national que supranational, d'obligations juridiques pour un accès à l'information sur demande et pour une mise à disposition active des informations. Ils plaident pour faire reconnaître la liberté d'information comme un droit fondamental international. En outre, ils recommandent que tous les États adhèrent à la Convention du Conseil de l'Europe sur l'accès aux documents publics du 18 juin 2009 (Convention de Tromsø). La Suisse figure parmi les États n'ayant pas encore adhéré à cette convention.

La «Déclaration de Berlin» se trouve sur notre site www.leprepose.ch, dans la rubrique Le PFPDT – Coopération internationale.

3. Le PFPDT

3.1 Huitième Journée de la protection des données

À l'occasion de la 8e journée internationale de la protection des données, nous avons organisé une table ronde consacrée aux révélations faites par Edward Snowden et à leurs conséquences pour la protection des données en Suisse. Les citoyens ont par ailleurs eu la possibilité de s'exprimer sur cette question sur notre blog.

La discussion, qui a eu lieu le 28 janvier 2014 au Forum politique de la Confédération (Käfigturm) à Berne, a réuni le Préposé fédéral à la protection des données et à la transparence Hanspeter Thür, la conseillère aux États socialiste Anita Fetz, le conseiller national libéral-radical Ruedi Noser et le président du Parti pirate Alexis Roussel. La table ronde était animée par René Zeller, rédacteur en chef adjoint de la NZZ. Les participants se sont accordés à dire que les révélations sur les agissements des services de renseignement américains (NSA) ont conféré une nouvelle dimension à la question de la protection de la sphère privée et qu'elles ont ouvert les yeux des politiques et du public.

Ils ont par ailleurs relevé que les services de renseignement et autres autorités n'étaient pas les seuls à collecter assidûment des données, mais que les entreprises privées n'étaient pas en reste. Il suffit de songer aux cartes de fidélité, aux réseaux sociaux, aux sites de vente aux enchères, aux transactions bancaires en ligne ou encore à l'«Internet des objets». L'utilisation de services et de technologies de ce type génère un nombre considérable de données personnelles («Big Data») qui peuvent être valorisées au moyen de méthodes raffinées. Ces dernières permettent en particulier de déterminer et de prévoir de manière précise le comportement des utilisateurs.

Alors que M. Noser a relevé l'utilité de ces volumes massifs de données, les autres participants se sont inquiétés des risques qui en découlent pour la sphère privée des utilisateurs et ont estimé qu'il fallait prendre des mesures, notamment en matière de transparence et en ce qui concerne le droit à l'autodétermination informationnelle. À cet égard, M. Thür a proposé que le PFPDT soit doté de pouvoirs supplémentaires pour sanctionner les violations.

Le même jour, des citoyens se sont exprimés sur notre blog concernant les conséquences de l'affaire Snowden dans le domaine de la protection des données.

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

Notre principal canal de publications est le site internet www.leprepose.ch sur lequel les citoyens trouvent des informations utiles concernant la protection des données et le principe de la transparence. Au cours de l'année sous revue, nous avons publié, entre autres, des commentaires relatifs à la vidéosurveillance, au webtracking, au monitoring des médias sociaux et aux contrôles antidopage.

Les caméras embarquées (dashcams) sont la dernière tendance en matière de vidéosurveillance. Installées sur des véhicules, elles permettent de filmer la route, que ce soit par simple divertissement ou pour disposer de preuves en cas d'accident. L'utilisation de ces caméras se heurte toutefois à certains principes en matière de protection des données. Des informations plus détaillées se trouvent sur notre site internet www.leprepose.ch à la rubrique Protection des données – technologies – vidéosurveillance.

La vidéosurveillance dans les vestiaires et dans les toilettes augmente sensiblement le risque d'une violation de la sphère intime. Dès lors, son emploi n'est autorisé dans ces espaces qu'à condition de respecter certaines règles strictes en matière de protection des données (voir nos explications dans la rubrique protection des données – technologies – vidéosurveillance). Dans la même rubrique nous avons publié des informations concernant la transmission d'enregistrements vidéo aux autorités de poursuite pénale et au sujet des drones.

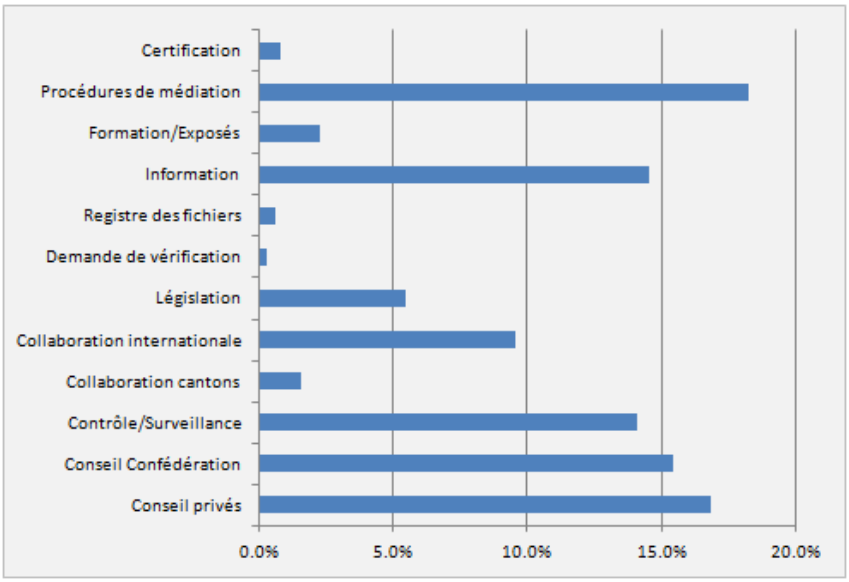
En outre, on trouve désormais sur notre site internet des commentaires à propos du monitoring des médias sociaux (protection des données – Internet et ordinateur – services en ligne - médias sociaux). Celui-ci permet d'assurer un suivi systématique et permanent des informations importantes concernant une entreprise qui sont publiées sur les réseaux sociaux en ligne.

Les exploitants de sites web et les réseaux publicitaires recourent au webtracking pour suivre les activités des visiteurs sur un site donné ou pour observer le comportement de navigation des internautes. Les données ainsi collectées permettent de tirer des conclusions quant aux intérêts, préférences ou habitudes des internautes. Or, comme nous l'expliquons sur notre site internet (protection des données – Internet et ordinateur – webtracking), nombre d' instruments de webtracking posent problème du point de vue de la protection des données.

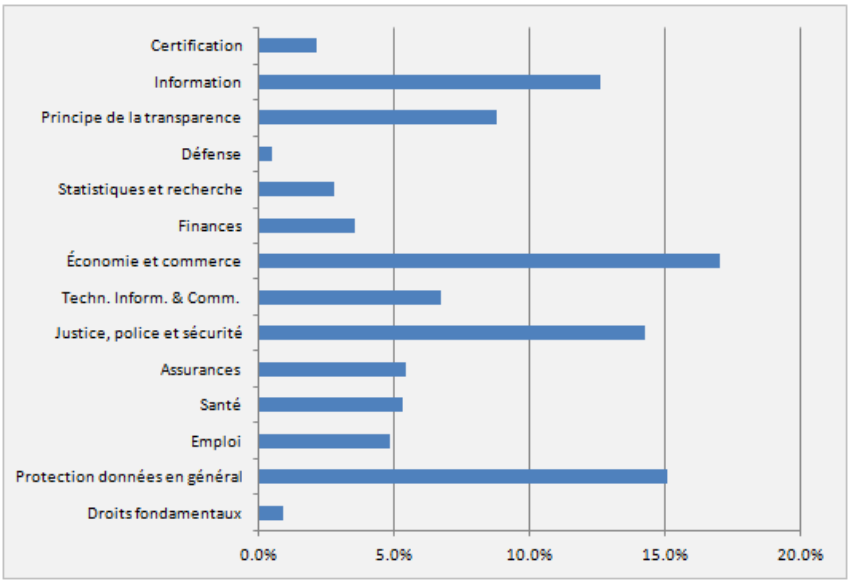
Enfin, nous avons publié des explications dans le domaine des contrôles antidopage (Protection des données – loisirs et sport – sport et dopage). Elles traitent de la loi fédérale sur l'encouragement du sport et de l'activité physique, entrée en vigueur en 2012, qui règle notamment les contrôles antidopage et l'échange de données entre les organes nationaux et internationaux de lutte contre le dopage.

3.3 Statistique des activités du PFPDT du 1er avril 2013 au 31 mars 2014

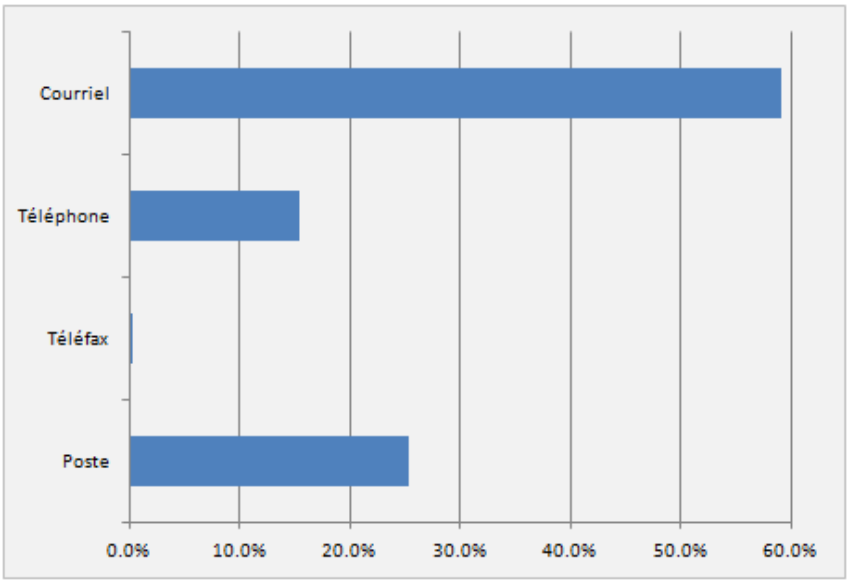
Charge de travail par tâches



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 2013 au 31 décembre 2013)

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
ChF	27	15	8	4	0	0
DFAE	73	63	5	5	0	0
DFI	92	39	18	29	4	2
DFJP	48	17	20	7	2	2
DDPS	29	6	17	5	0	1
DFF	32	11	13	8	0	0
DEFR	68	19	18	28	0	3
DETEC	100	48	23	17	2	10
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 %)	-	-
Total 2007 (en %)	249 (100 %)	147 (59 %)	82 (33 %)	20 (8 %)	-	-

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
ChF	13	5	7	1	0	0
PFPDT	14	10	1	3	0	0
Total	**27**	**15**	**8**	**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	73	63	5	5	0	0
Total	**73**	**63**	**5**	**5**	**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	12	3	1	8	0	0
BFEG	0	0	0	0	0	0
OFC	7	4	0	3	0	0
AFS	4	4	0	0	0	0
METEO CH	0	0	0	0	0	0
BN	0	0	0	0	0	0
OFSP	33	15	5	10	3	0
OFS	1	0	0	1	0	0
OFAS	13	7	5	1	0	0
OVF*	4	4	0	0	0	0
MNS	0	0	0	0	0	0
SWISS-MEDIC	18	2	7	6	1	2
SUVA	0	0	0	0	0	0
Total	**92**	**39**	**18**	**29**	**4**	**2**

* depuis le 1er janvier 2014 Office fédéral de la sécurité alimentaire et des affaires vétérinaires OSAV

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	5	2	2	1	0	0
OFJ	3	2	0	1	0	0
FEDPOL	4	2	1	1	0	0
METAS	2	1	1	0	0	0
ODM	24	9	12	0	2	1
ISDC	0	0	0	0	0	0
IPI	1	0	1	0	0	0
CFMJ	5	1	0	3	0	1
CAF	0	0	0	0	0	0
ASR	0	0	0	0	0	0
CSI	4	0	3	1	0	0
CNPT	0	0	0	0	0	0
Total	**48**	**17**	**20**	**7**	**2**	**2**

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	6	3	2	1	0	0
Défense/ armée	3	0	3	0	0	0
SRC	12	1	8	3	0	0
arma-suisse	7	1	4	1	0	1
OFSPO	0	0	0	0	0	0
OFPP	1	1	0	0	0	0
Total	**29**	**6**	**17**	**5**	**0**	**1**

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	7	2	3	2	0	0
AFF	2	1	1	0	0	0
OFPER	2	0	2	0	0	0
AFC	5	0	4	1	0	0
AFD	4	3	1	0	0	0
RFA	2	0	1	1	0	0
OFCL	2	1	0	1	0	0
OFIT	1	0	0	1	0	0
CDF	6	4	0	2	0	0
SFI	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
CdC	0	0	0	0	0	0
Total	**32**	**11**	**13**	**8**	**0**	**0**

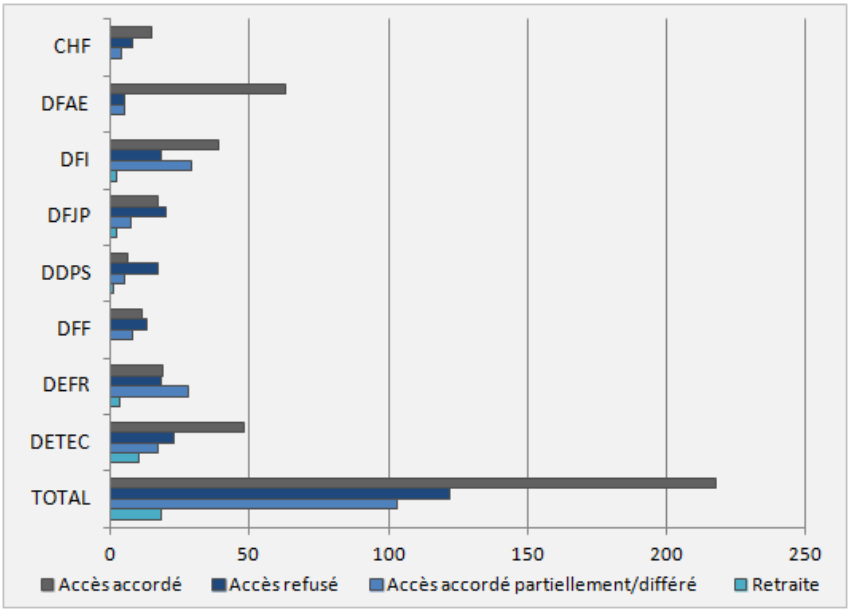
Département fédéral de l'économie, de la formation et de la recherche DEFR

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	0	0	2	0	0
SECO	9	3	3	3	0	0
SEFRI	4	0	4	0	0	0
OFAG	30	4	7	19	0	0
OFAE	1	0	1	0	0	0
OFL	0	0	0	0	0	0
SPr	2	1	1	0	0	0
COMCO	16	8	2	3	0	3
ZIVI	0	0	0	0	0	0
BFC	0	0	0	0	0	0
FNS	1	0	0	1	0	0
IFFP	0	0	0	0	0	0
CEPF	3	3	0	0	0	0
Total	**68**	**19**	**18**	**28**	**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	7	2	1	4	0	0
OFAC	17	10	6	1	0	0
OFEN	11	5	3	3	0	0
OFROU	4	4	0	0	0	0
OFCOM	5	1	0	1	0	3
OFEV	14	6	3	5	0	0
ARE	1	1	0	0	0	0
ComCom	1	1	0	0	0	0
IFSN	26	6	10	3	0	7
PostCom	0	0	0	0	0	0
AIEP	14	12	0	0	2	0
Total	**100**	**48**	**23**	**17**	**2**	**10**

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 2013 au 31 décembre 2013)

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	1	0	1	0	0	0
Total	**1**	**0**	**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 2013 au 31 décembre 2013)

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	0	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**	**0**

3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2013 au 31 décembre 2013)

Catégorie de requérants	2013
Médias	24
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	27
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	8
Avocats	11
Entreprises	6
Universités	0
Total	**76**

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:	5 personnes
Chancellerie:	2 personnes