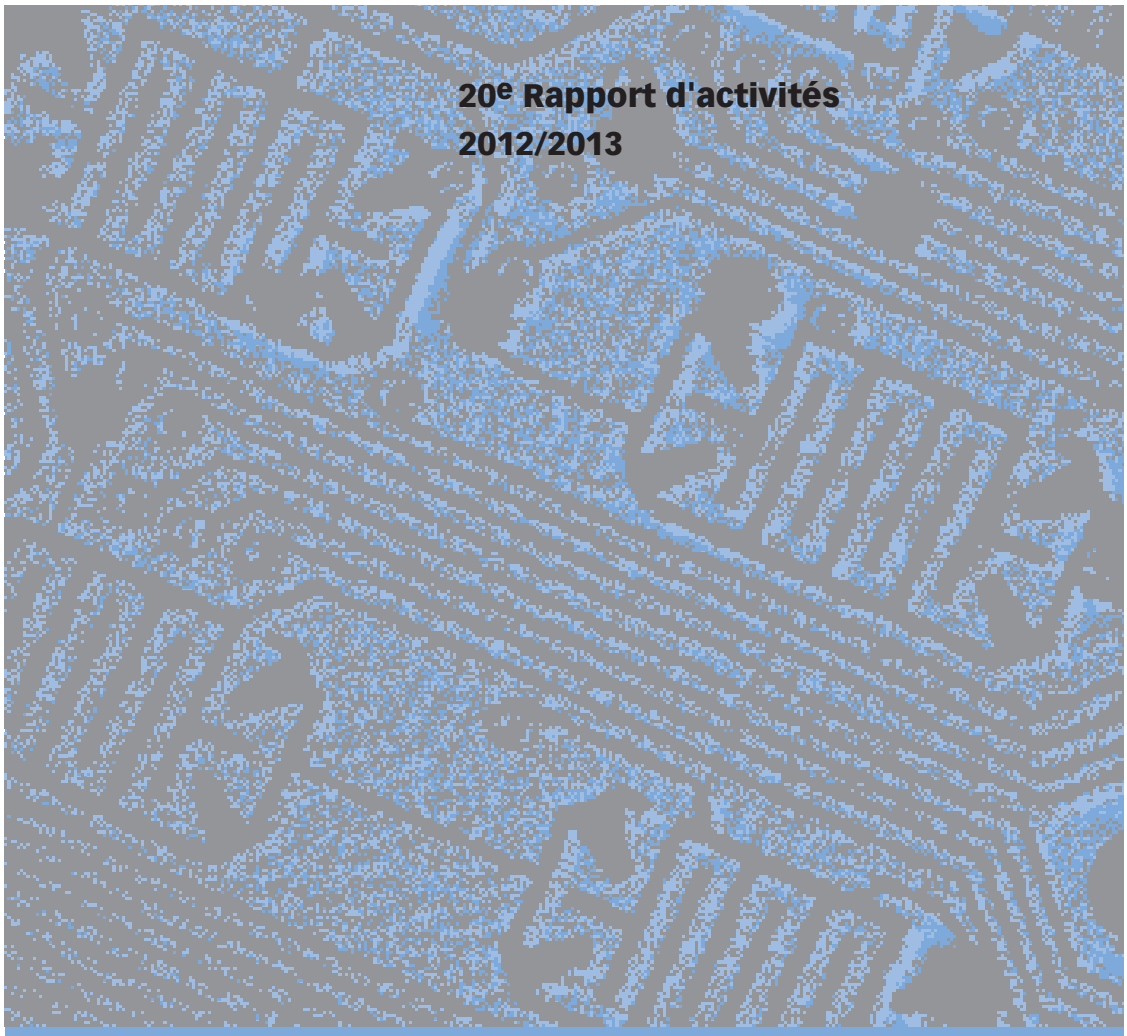


20e Rapport d'activités 2012/2013

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2012/2013 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 2012 au 31 mars 2013.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.020.d/f

Table des matières

Avant-propos – Bilan et perspectives 7
Liste des abréviations 12
1. Protection des données 16
1.1 Droits fondamentaux 16
1.1.1 Aspects du traitement de données dans le cadre des relevés statistiques 16
1.1.2 Introduction du numéro AVS dans le registre foncier 17
1.1.3 Utilisation du numéro AVS dans la loi sur la TVA 18
1.1.4 Thinkdata.ch: actualisation et développement 18
1.2 Protection des données – Questions d'ordre général 20
1.2.1 Vidéosurveillance dans les vestiaires de centres de loisir 20
1.2.2 Stockage centralisé de photos de clients dans les stations de ski 22
1.2.3 Voyageurs sans titre de transport valable – contrôle de la base de données auprès des CFF 22
1.2.4 Dispositions d'exécution concernant la législation dans le domaine du sport 25
1.2.5 Traitement de données personnelles en relation avec des manifestations sportives 26
1.2.6 Lutte contre le dopage et communication de données personnelles à l'étranger 27
1.2.7 Tour d'horizon des technologies biométriques 28
1.2.8 Formation concernant l'élaboration d'un règlement de traitement 29
1.3 Internet et télécommunication 31
1.3.1 Explications concernant les mises au pilori sur internet 31
1.3.2 Prises de vue des voies publiques sur Internet – Arrêt du Tribunal fédéral 32
1.3.3 Echange de contenus sur internet – situation juridique après l'arrêt Logistep 33
1.3.4 Plateforme immobilière sur Internet 35
1.3.5 Monitoring des réseaux sociaux et protection des données 35
1.3.6 Utilisation d'outils d'analyses de l'audience internet pour les organes de la Confédération 36
1.3.7 Révision de la loi sur les publications officielles 37
1.3.8 Révision de l'ordonnance GEVER 38

1.4 Justice/Police/Sécurité ... 40
1.4.1 Mise en œuvre Schengen: évaluation de la protection des données dans les Etats baltes ... 40
1.4.2 Mise en œuvre Schengen: signalements de personnes dans le SIS en vue de l'arrestation aux fins d'extradition ... 41
1.4.3 Mise en œuvre Schengen: information aux utilisateurs et mention légale lors des accès RIPOL, SIS et SYMIC ... 42
1.4.4 Accords avec les Etats-Unis pour le maintien de la Suisse dans le Visa Waiver Program ... 43
1.4.5 Révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication ... 44
1.4.6 Loi sur le renseignement ... 45
1.4.7 Recherche de véhicules et surveillance de la circulation automatisées ... 46
1.4.8 Droit d'accès aux données du système d'information ISIS: ancien et nouveau mécanisme ... 48
1.4.9 Essai pilote du système d'information ISAS ... 48
1.4.10 Loi sur la sécurité de l'information: Participation au groupe de travail FOGIS ... 50
1.5 Santé et recherche ... 52
1.5.1 SwissDRG: certification des nouveaux services de réception de données ... 52
1.5.2 Cybersanté suisse et le dossier électronique du patient: état actuel des développements ... 54
1.5.3 Implications de la vente de médicaments par correspondance sur la protection des données ... 55
1.5.4 Règlement de traitement des données des assurances: obligation de transmettre au PFPDT ... 57
1.5.5 Projet de loi fédérale sur l'enregistrement du cancer et autres maladies ... 58
1.5.6 Activité de surveillance dans le domaine de la recherche médicale ... 60
1.6 Assurances ... 63
1.6.1 Procédure d'établissement des faits auprès d'un assureur-maladie ... 63
1.6.2 Sondage sur le don d'organes par une assurance ... 64
1.7 Secteur du travail ... 67
1.7.1 Exigences envers un système pour lanceurs d'alertes ... 67
1.7.2 Envoi de certificats de caisse de pension – arrêt du Tribunal administratif fédéral et suivi du contrôle ... 68

1.7.3 Communication aux autorités américaines de données concernant des collaborateurs ... 69
1.7.4 Systèmes de surveillance et de contrôle sur le lieu de travail ... 71
1.7.5 Gestion du compte de messagerie dans la vie professionnelle ... 72
1.7.6 Assurance qualité conforme à la protection des données dans un institut privé d'études de marché ... 74
1.7.7 Code de comportement visant à prévenir les conflits d'intérêts des employés fédéraux ... 75
1.8 Economie et commerce ... 77
1.8.1 Analyse du panier pour les programmes de fidélisation des clients ... 77
1.8.2 Contrôle dans le domaine des agences de renseignement économique et de renseignement en matière de crédit: Moneyhouse ... 78
1.8.3 Envoi de pièces justificatives du registre du commerce par internet ... 79
1.8.4 Modernisation du registre du commerce – Modification du code des obligations ... 81
1.8.5 Traitement de données personnelles dans le commerce d'adresses ... 82
1.8.6 Ouverture du marché de la poste: révision totale de l'ordonnance ... 83
1.8.7 Base de données d'un prestataire de services financiers en relation avec des évènements relevant de la sécurité ... 85
1.9 International ... 86
1.9.1 Coopération internationale ... 86
2. Principe de la transparence ... 97
2.1 Demandes d'accès ... 97
2.1.1 Départements et offices fédéraux ... 97
2.1.2 Services parlementaires ... 98
2.1.3 Ministère public de la Confédération ... 98
2.2 Demandes en médiation ... 99
2.3 Procédures de médiation closes ... 100
2.3.1 Recommandations ... 100
2.3.2 Médiations ... 110
2.4 Décisions judiciaires relatives à la loi sur la transparence ... 111
2.4.1 Tribunal administratif fédéral ... 111
2.5 Consultation des offices et autres prises de position ... 113
2.5.1 Entrée en vigueur du nouveau droit comptable ... 113
2.5.2 Interpellation urgente: Halte à l'extension rampante du champ d'application des conventions collectives aux entreprises d'autres branches ... 113

2.5.3 Définition des nouveaux tarifs des analyses de laboratoire: transparence renforcée dans la procédure ... 113
2.5.4 Projet de loi sur le renseignement ... 114
2.6 Divers ... 116
2.6.1 Journée sur la transparence ... 116
2.6.2 Relations avec les services de conciliation – Groupe de travail sur la Médiation ... 116
3. Le PFPDT ... 117
3.1 La septième Journée de la protection des données ... 117
3.2 Publications du PFPDT au cours de l'exercice écoulé ... 118
3.3 Participation au Conseil informatique et au Comité pour la sécurité informatique de la Confédération ... 120
3.4 Sensibilisation et formation auprès des étudiants ... 122
3.5 Formation pour les conseillers en matière de protection des données dans l'administration fédérale ... 123
3.6 Statistique des activités du PFPDT du 1er avril 2012 au 31 mars 2013 ... 124
3.7 Statistique des demandes d´accès présentées auprès des départements en vertu de l´art. 6 de la loi sur la transparence (Période: 1er janvier 2012 au 31 décembre 2012) ... 127
3.8 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 2012 au 31 décembre 2012) ... 136
3.9 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 2012 au 31 décembre 2012) ... 137
3.10 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2012 au 31 décembre 2012) ... 138
3.11 Secrétariat du PFPDT ... 139

Avant-propos – Bilan et perspectives

Percée dans le domaine des identificateurs personnels et dans le dossier de la santé – Big data et surveillance généralisée, deux nouveaux défis

Il y a dix ans, nous nous sommes intéressés de près au projet d'un identificateur personnel. Il entendait harmoniser les registres, afin de permettre à l'avenir le recensement de la population sur la base du registre des habitants. Notre critique avait porté sur le fait que le but de cet identificateur biunivoque n'était pas suffisamment défini. Le numéro devait également servir des fins administratives pour lesquelles la description de l'utilisation qui allait en être faite était insuffisante. Notre proposition d'établir des numéros spécifiques à chaque domaine n'a malheureusement pas été retenue. Entre-temps, le nouveau numéro AVS a été créé. Son champ d'application est décrit de manière très large dans la loi (art. 50e LAVS). Depuis, l'utilisation de ce numéro s'est étendue: des administrations cantonales entières l'utilisent et de nouveaux besoins sont annoncés en permanence. Au départ, il était évident que le numéro AVS allait aussi être utilisé pour les dossiers électroniques des patients. Pascal Couchepin, alors chef du département en charge de cette question, avait pris cette décision fondamentale bien que nous ayons, à l'époque, clairement fait part de nos préoccupations à ce sujet: d'une part, concernant la large diffusion de ce numéro (emploi, formation, fiscalité, etc.) et d'autre part, par rapport à l'intention de l'utiliser de manière encore plus étendue. Dès lors, on ne pouvait et on ne peut plus guère parler de numéro anonyme, ce qui était pourtant la prémisse de base. À la suite du changement à la tête du département, et malgré ladite décision, nous avons saisi l'occasion de remettre cette question à l'ordre du jour. Ce qui a porté ses fruits. Une percée considérable fut opérée. Ainsi, le Conseil fédéral est désormais d'accord pour que la Centrale de Compensation (CdC) crée un numéro d'identification électronique du patient selon un mode aléatoire et qu'elle le sauvegarde avec le numéro AVS. Nous sommes d'avis qu'à l'avenir, la CdC pourrait aussi produire des numéros spécifiques dans d'autres domaines délicats, par exemple le vote électronique.

A cet endroit, je voudrais signaler un progrès important dans le domaine de la santé. Des années durant, nous avons critiqué le fait que bien trop de données médicales, qui n'étaient pas absolument indispensables, circulaient entre les fournisseurs de prestations et les assurés. Pour cette raison, nous avons à nouveau demandé aux assurances-maladie de nous expliquer en détail comment le contrôle des factures se déroule dans la pratique. En lieu et place d'informations détaillées, nous avons à chaque fois reçu la même réponse stéréotypée: afin de

pouvoir juger de l'efficacité, de l'opportunité et du caractère économique d'une mesure, les caisses auraient besoin de toutes les données disponibles sur les patients! Or, nous savions d'ores et déjà que la majorité des factures étaient examinées automatiquement, puis remboursées sans plus de contrôle. Dans la perspective de l'introduction des forfaits par cas (SwissDRG), le risque était que d'énormes quantités de données médicales numérisées s'amoncèlent auprès des assurances. La proposition que nous faisons depuis des années de mettre en place, entre le prestataire et l'assuré, un service de réception des données indépendant et certifié qui détermine, sur la base d'un triage automatique, quelles factures doivent être examinées de plus près, s'est retrouvé soudainement au cœur des débats grâce au soutien du Conseiller fédéral Alain Berset et a fini par être intégrée dans l'ordonnance du Conseil fédéral. Nous sommes persuadés que ce système permet d'améliorer sensiblement la protection de la personnalité dans le domaine de la santé, même s'il n'est pas encore appliqué partout et si certains points nécessitent des éclaircissements.

Nous sommes heureux qu'au cours de l'année 2012, soit six ans après l'entrée en vigueur de la loi sur la transparence (LTrans), le personnel prévu dans le message nous ait enfin été attribué. Certes, la montagne de dossiers accumulés ne pourra pas être éliminée d'un coup. Toutefois, nous espérons qu'une bonne partie des quelques 75 cas qui n'ont pas pu être réglés à la fin 2012 dans les délais prescrits par la loi pourra être traitée en 2013. Au cours de l'exercice écoulé, une mise au point importante a été faite en ce qui concerne la LTrans: nombres de services tentent de s'extraire du champ d'application de cette loi, en argumentant qu'ils ne pourraient autrement pas assumer suffisamment leurs tâches. Même le Contrôle fédéral des finances (CDF) l'a demandé, craignant de ne plus pouvoir accéder à des informations importantes si les informateurs se méfient de la transparence. Nous nous y sommes opposés avec l'argument suivant: il est contradictoire qu'une autorité de surveillance dont la tâche est d'établir la transparence sur les éventuels dysfonctionnements de l'administration ne soit pas tenue d'être elle-même transparente sur sa propre activité. Entre-temps, le Conseil fédéral s'est rallié à ce point de vue et a rejeté la demande de révision du CDF. D'autres tentatives de ce type sont en suspens contre lesquelles nous nous prononcerons, car nous estimons que, notamment les services de renseignements et la commission de la concurrence sont tenus de faire preuve de transparence vis-à-vis des citoyens.

Au cours de l'exercice écoulé, nous avons procédé à de nombreux examens des faits portant sur des questions centrales (p.ex. vidéosurveillance dans les vestiaires, sociétés de renseignements commerciaux) et avons, dans le cadre de la consultation des offices, pris position sur des lois importantes (p.ex. LSCPT,

LMSI, registre du commerce électronique et ordonnance sur la poste). Nos remarques et critiques ont été prises en compte dans une large mesure à propos de la réglementation du cheval de Troie gouvernemental, mais aussi concernant la question de régler au niveau légal et de manière restrictive les cas où une ingérence du service de renseignement dans la vie privée peut être admise. Nous espérons que les quelques points encore ouverts seront réglés au cours des délibérations parlementaires. Par ailleurs, la modification de l'ordonnance sur la poste a été pour nous l'occasion de présenter une exigence qui nous tient à cœur depuis longtemps: à partir de la fin de l'année 2012, la poste ne peut plus facturer les 30 francs de frais aux clients qui ne sont pas d'accord pour que leur demande de réexpédition soit transmise à des tiers. La communication de la poste entourant cette demande de réexpédition est elle aussi plus transparente: dorénavant, une liste détaillée sera établie énumérant les destinataires des adresses, par exemple les commerçants d'adresses, les sociétés de renseignements commerciaux, les assurances, les banques, etc. Dès lors, un consentement global pour qu'une transmission à des tiers soit permise n'est plus suffisant dans ce cas.

Enfin, nous avons publié sur notre site internet des commentaires et des informations concernant divers thèmes, par exemple la mise au pilori sur la toile, la protection des données dans le contexte des manifestations sportives destinées au grand public ainsi que l'utilisation par des organes fédéraux d'outils d'analyse pour les sites internet. Une brochure traitant de la protection des données sur le lieu de travail a également été édité par nos soins.

En 2012, les sociétés de renseignements commerciaux et le commerce des adresses, qui préoccupent particulièrement le PFPDT, se sont révélés être des nouveaux chantiers de grande ampleur. Tout a démarré lorsque des particuliers se sont aperçus, par une recherche sur Google, qu'ils figurent sur le site d'une société de renseignements commerciaux avec de nombreuses informations allant jusqu'à la personne avec laquelle ils cohabitent et à l'indication de leur solvabilité. Le choc a été particulièrement grand pour celles et ceux qui, bien qu'ayant bloqué leur adresse auprès de leur opérateur téléphonique ou auprès de la poste, ont constaté qu'ils figurent avec leur adresse complète sur internet. Nous avons réagi immédiatement et réussi à faire imposer par le biais d'une mesure provisoire que la protection des personnes concernées, qui ne veulent pas publier leur adresse pour des raisons de sécurité, soit immédiatement améliorée. Au cours d'une procédure complexe d'établissement des faits, nous avons fait la lumière sur la question des flux de données concernant la société de renseignements commerciaux examinée et avons exigé d'elle, sur la base d'une série de recommandations, un traitement garantissant le respect des droits de la personnalité. Ces recommandations

valent naturellement pour tous les acteurs de la branche. Nous examinerons de très près comment elles seront mises en pratique et interviendrons si nécessaire par des mesures complémentaires. Cette première clarification a mis l'accent uniquement sur la gestion des adresses bloquées, mais a aussi fait ressortir une foule de problèmes et de questions qui demandent un examen plus approfondi. La question centrale est de savoir comment des données provenant de diverses sources et traitées à des fins différentes sont rassemblées, recomposées et analysées, et comment les résultats ainsi obtenus peuvent être publiés sur internet sans le consentement des personnes concernées. Quoi qu'il en soit, une grande incompréhension règne parmi les personnes qui nous ont demandé conseil lorsqu'elles se voient contraintes d'accepter qu'énormément de détails les concernant soient consultables sur internet. Sans vouloir préjuger du résultat de nos recherches, je peux d'ores et déjà me permettre de dévoiler une conclusion importante: dans le domaine des sociétés de renseignements commerciaux, du commerce d'adresses et notamment de la publication de données personnelles sur internet, la situation juridique est actuellement lacunaire, à tel point qu'un remaniement profond de la loi sur la protection des données s'impose.

La protection des données n'est pas seulement mise à rude épreuve par internet. A l'avenir nous serons confrontés à des innovations technologiques ainsi qu'à des produits qui permettront un contrôle total et une surveillance permanente de notre vie sociale, tant de la part des entreprises privées que des pouvoirs publics. Le Maire de New York n'a-t-il pas approuvé l'intervention de drones militaires qui, situés à très haute altitude, seraient capables de saisir chaque détail dans le but de surveiller la Métropole? Ainsi, une personne qui lit, sur un banc, devra s'attendre à ce que le drone (c'est-à-dire la personne qui se cache derrière) lise avec elle. L'utilisation de très petits aéronefs dotés à peu de frais d'une technologie dernier cri permettra à tout individu un tant soit peu curieux de procéder à des vols de reconnaissance à une distance proche ou plus éloignée, de regarder à l'intérieur de locaux et peut-être même de se glisser par une fenêtre ouverte. Les différentes technologies informatiques rendant possible le phénomène de la «réalité augmentée» nous permettrons non seulement de percevoir la réalité à travers nos lunettes et de la remettre en question, mais également de la comparer et de l'interpréter avec toutes les informations figurant en ligne. Bientôt, peut-être, un passant doté de «Google Glass» vous saluera-t-il par votre nom alors que vous flânez avec votre amie dans les rues de Londres au cours d'un week-end prolongé. Ses lunettes auront pris une photo de vous, l'auront comparée avec les images disponibles sur internet et – grâce au procédé de la reconnaissance faciale - vous aura identifié. Quelle sympathique rencontre, n'est-ce pas?

Le thème de la gestion massive de données (« big data ») est aussi un sujet de plus en plus actuel. D'énormes quantités de données sont:

- générées automatiquement (liaisons de télécommunication, accès internet, « logfiles »),
- saisies automatiquement par des lecteurs RFID, des caméras, des microphones ou autres appareils,
- issues de transactions financières ou
- produites dans le secteur de la santé, de l'énergie, etc.

Compte tenu du progrès technique, des énormes capacités de stockage, de la possibilité de transmettre rapidement de gros volumes d'informations sur de grandes distances ainsi que de la précision d'analyse de ces informations, les données deviennent une véritable matière première (le « nouveau capital ») dans une société future dirigée par les données (« data driven » Alex Pentland, professeur d'informatique au Massachusetts Institute of Technology). Les algorithmes permettent d'obtenir, à partir de ces masses de données, des résultats encore jamais atteints dont la conséquence représente un danger sans nom pour la sphère privée. Voici quelques exemples: lorsque l'analyse d'un grand nombre de données permet de conclure qu'une femme mariée qui achète soudainement un bijou de grande valeur se trouve en général à la veille d'une séparation ou que l'analyse des données relatives aux transactions du client d'une banque permet d'établir que le client en question pourrait bientôt mourir, il est évident qu'il y a là un potentiel d'abus. Dans ce contexte et dans la perspective du débat sur la révision de la loi, se pose la question de savoir si l'on peut maîtriser par des lois ces grandes quantités de données ou leur utilisation potentielle de manière exhaustive.

D'une manière générale, la gamme de services internet ne cesse d'augmenter due à la masse de données disponibles. Par voie de conséquence, nous pouvons nous interroger sur comment maîtriser cette évolution dans un cadre législatif national.

Liste des abréviations

ACC	Autorité de contrôle commune de Schengen
AFC	Administration fédérale des contributions
AFD	Administration fédérale des douanes
AFAPDP	Association francophone des autorités de protection des données
AMA	Agence Mondiale Antidopage
ASR	Autorité fédérale de surveillance en matière de révision
ATF	Arrêts du Tribunal fédéral
CAAS	Convention d'application de Schengen
CCT	Convention collective de travail
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CdG-N	Commission de gestion du Conseil national
CEPD	Contrôleur Européen à la protection des données
ChF	Chancellerie fédérale
CI	Conseil informatique (de la Confédération)
COMCO	Commission de la concurrence
C-SI	Comité de la sécurité informatique
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
DélFin	Délégation des finances
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
DFI	Département fédéral de l'intérieur
DRG	Diagnoses Related Groups
EPFZ	Ecole Polytechnique Fédérale de Zurich

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
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
FNS	Fonds national suisse de la recherche scientifique
FOGIS	Formell-gesetzliche Grundlage für den Informationsschutz (Base légale formelle pour la protection de l'information)
GEVER	Gestion électronique des affaires (Elektronische Geschäftsverwaltung)
GEWA	Système d'information pour la lutte contre le blanchiment d'argent, la criminalité organisée et le financement du terrorisme
HSPD-6	Homeland Security Presidential Directive 6
IFSN	Inspection fédérale de la sécurité nucléaire
ISAS	Système d'information sécurité extérieure
ISIS	Système d'information sécurité intérieure
JANUS	Système informatisé de la Police judiciaire fédérale
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LDEP	loi fédérale sur le dossier électronique du patient
LESp	Loi fédérale sur l'encouragement du sport et de l'activité physique
LFRC	Loi fédérale sur le renseignement civil
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LPD	Loi fédérale sur la protection des données
LPers	Loi fédérale sur le personnel de la Confédération
LRens	Loi fédérale sur le renseignement
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LSF	Loi fédérale sur la statistique fédérale

LTrans	Loi fédérale sur le principe de la transparence dans l'administration
LTV	Loi fédérale sur le transport de voyageurs
LTVA	Loi fédérale régissant la taxe sur la valeur ajoutée
MC	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
OCPD	Ordonnance sur les certifications en matière de protection des données
ODM	Office fédéral des migrations
OFAC	Office fédéral de l'aviation civile
OFAS	Office fédéral des assurances sociales
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
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
OGEmol	Ordonnance générale sur les émoluments
OIAF	Ord. sur l'informatique dans l'administration fédérale
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
ONCR	Ordonnance sur les normes comptables reconnues
OPers	Ordonnance sur le personnel de la Confédération
ORFC	Office fédéral du registre du commerce
OSRev	Ordonnance sur la surveillance de la révision
OTrans	Ordonnance sur le principe de la transparence dans l'administration

PCSC	Cooperation in Preventing and Combating Serious Crime
PFPDT	Préposé fédéral à la protection des données et à la transparence
RIPOL	Système de recherches informatisées de police
RogF	Reisende ohne gültigen Fahrausweis (Système d'information Voyageurs sans titre de transport valable)
RSA	Recherche de véhicules et surveillance de la circulation automatisées
SECO	Secrétariat d'Etat à l'économie
SIS	Système d'information Schengen
SRC	Service de renseignements de la Confédération
Swissmedic	Institut suisse des produits thérapeutiques
SYMIC	Système d'information central sur la migration
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TIC	Technologies de l'information et de la communication
UPIC	Unité de pilotage informatique de la Confédération
VIS	Système d'information sur les visas
Zefix	Index central des raisons de commerce

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Aspects du traitement de données dans le cadre des relevés statistiques

Début 2012, nous avons été amenés à donner notre avis dans le cadre d'un projet de modification de l'ordonnance concernant l'exécution des relevés statistiques fédéraux et de l'élaboration d'un règlement sur l'appariement des données au sein de l'Office fédéral de la statistique. Nous avons pris position sur ces deux projets et participé à plusieurs séances. Dans l'ensemble nos remarques ont été bien accueillies. Si les travaux législatifs entrepris tendent à une plus grande transparence ainsi qu'à l'inclusion des aspects de protection des données, certains sujets devraient faire l'objet de précisions supplémentaires.

En 2012, l'Office fédéral de la statistique (OFS) a élaboré un projet de révision relatif à l'ordonnance concernant l'exécution des relevés statistiques fédéraux de même qu'un projet de règlement de traitement sur l'appariement des données. Ladite ordonnance prévoit, notamment un nouveau chapitre sur l'appariement des données ainsi que des précisions sur leur traitement. Afin de s'assurer que la protection des données personnelles soit garantie au sein de ce projet, l'OFS nous a invité à participer à plusieurs séances.

Nous avons fait part de notre position à l'OFS tout en saluant, dans l'ensemble, le travail juridique entrepris par ce dernier ainsi que les efforts d'y inclure les aspects de protection des données. Nous avons également constaté la transparence prévue dans le traitement de données ainsi que l'indication des mesures de pseudonymisation et d'anonymisation. Il conviendrait selon nous, notamment de préciser dans le texte de l'ordonnance quel est le matériel effectivement détruit (en principe celui à l'origine de la collecte des données, tel que les questionnaires et autres documents d'enquête) et dans quel laps de temps. De même, le moment auquel intervient l'anonymisation des données statistiques devra être également davantage précisé (en effectuant une distinction par catégorie si nécessaire).

Nous saluons également l'élaboration d'un règlement de traitement sur l'appariement des données traitant notamment des aspects importants de protection des données, tels que le but de ce traitement, la pseudonymisation des données, les précisions sur le processus d'appariement, l'accès aux données, etc.

En l'état, le règlement ne donne en revanche que des informations peu détaillées sur les mécanismes à mettre en œuvre. L'OFS entend continuer à développer les différents points qui y sont abordés et nous soumettra, conformément à notre demande, prioritairement le chapitre sur le «Key Management» (gestion des clés), lequel devrait être selon nous effectué par un organe indépendant, disposant des ressources et des compétences nécessaires et dont le processus constitue une préoccupation centrale du point de vue de la protection des données, au même titre que ceux de l'anonymisation et de l'effacement des données appariées.

Nous appuyons l'OFS dans la mise en place de ressources supplémentaires à des fins de contrôles internes relatifs aux traitements de données effectués dans le cadre de la mise en œuvre des dispositions de la loi fédérale sur la statistique et de la législation fédérale sur la protection des données.

Nous avons également pris note de l'intérêt de l'OFS à la certification du Key Management. A cette fin, il a préalablement été rendu attentif à l'investissement conséquent qu'un tel processus requiert. En outre, il ne pourrait s'agir en l'espèce, que d'une certification portant sur l'organisation et la procédure liée au Key Management au sens de l'article 4 de l'ordonnance sur les certifications en matière de protection des données (OCPD) à défaut de la certification du produit même.

1.1.2 Introduction du numéro AVS dans le registre foncier

Le numéro AVS sera introduit dans le registre foncier. Toutefois, il ne sera visible qu'à l'interne.

Il est prévu d'introduire le numéro AVS dans le registre foncier à titre d'identifiant supplémentaire des personnes. Nous nous sommes prononcés à ce sujet dans le cadre d'une consultation des offices. Nous avons approuvé à cette occasion l'intention du projet de ne permettre la consultation du numéro d'AVS qu'au niveau interne afin d'empêcher l'établissement indésirable de profils de fortune par des particuliers. Nous avons toutefois souligné que le cercle des personnes autorisées à y accéder n'était pas décrit avec suffisamment de précision dans le projet de loi qui nous a été soumis.

D'une manière générale, suite à la création des bases légales nécessaires, le numéro AVS sera aussi introduit, pendant l'exercice en cours, dans plusieurs autres domaines, à savoir le registre du commerce, Infostar et celui de la TVA (cf. ch. 1.1.3 du présent rapport d'activités. Pour ce qui est des dossiers électroniques des patients, une autre solution a été choisie (cf. ch. 1.5.2 du présent rapport d'activités).

1.1.3 Utilisation du numéro AVS dans la loi sur la TVA

L'Administration fédérale des contributions nous a soumis, de sa propre initiative, son projet d'amélioration de la législation sur le traitement des numéros AVS du point de vue de la protection des données. Ces améliorations concernant aussi une procédure de traitement automatisé des données.

Nous nous sommes à plusieurs reprises prononcés par le passé, dans le cadre de la consultation des offices, en faveur d'une amélioration urgente des bases légales de la TVA. D'une part concernant l'utilisation du numéro AVS qui n'était réglementée qu'au niveau de l'ordonnance (cf. notre 19e rapport d'activités 2011/2012, ch.1.9.3). Et d'autre part, au sujet du manque de précision de l'article 76 de la loi sur la TVA (LTVA) qui régit le procédé automatisé de consultation. L'Administration fédérale des contributions nous a contacté au cours de l'exercice écoulé et nous a présenté un projet de remaniement de l'article 76 LTVA. Il a été tenu compte des réserves que nous avions émises: la procédure d'appel a été réglementée de manière plus précise et l'utilisation des numéros AVS est désormais régie au niveau de la loi.

1.1.4 Thinkdata.ch: actualisation et développement

Après le lancement du service Thinkdata.ch – un service de sensibilisation à la protection des données et à la transparence à l'intention des organisations – en janvier 2012, les activités du groupe de travail ont continué durant l'année écoulée. Elles ont permis la mise en production de la deuxième version du service qui est désormais disponible en quatre langues.

Nous soutenons toujours le service Thinkdata.ch en participant de manière active au groupe de travail qui le développe. Le service a rencontré un succès important dès sa mise en fonction en janvier 2012. En mai 2012, une rencontre autour du service et de son futur a été organisée à Genève. Une trentaine de personnes d'horizons variés y ont participé. En plus d'initier la réflexion sur les versions à venir, ceci a permis au groupe de travail de se renforcer avec l'arrivée de nouveaux membres.

Le service a été enrichi de plusieurs nouveaux scénarios grâce à la participation des utilisateurs du site qui ont la possibilité d'envoyer leurs propres exemples de problématiques relatives à la protection des données et à la transparence. Depuis juillet 2012, une version allemande du service est disponible. Depuis janvier 2013, les versions italienne et anglaise sont également en ligne. Peu avant cette nouvelle

extension du service, le cap des 10 000 visites sur le site a été franchi. Chaque visite dure en moyenne plus de trois minutes.

Actuellement, le groupe de travail se penche sur le développement futur du service en se concentrant essentiellement sur les aspects internationaux. Ceci, afin de rendre son utilisation possible dans divers pays soumis à des ordres juridiques divergents. Parallèlement, nous définissons les lignes directrices de l'avenir opérationnel du service.

1.2 Protection des données – Questions d'ordre général

1.2.1 Vidéosurveillance dans les vestiaires de centres de loisir

Suite à des interpellations de citoyens, nous avons dû constater que de plus en plus d'exploitants de centres de loisir installent des caméras de surveillance dans des endroits sensibles tels que les vestiaires et les toilettes. Cette tendance est extrêmement inquiétante, du point de vue de la protection des données, puisqu'elle constitue une violation de la sphère privée des personnes concernées.

Le fait de filmer dans des vestiaires ou toilettes viole l'intimité des personnes concernées et porte ainsi atteinte à leur personnalité. Même si ces mesures de surveillance sont souvent prises pour des raisons compréhensibles – en règle générale pour prévenir ou sanctionner les vols – de telles atteintes à la personnalité sont difficilement justifiables. Cela signifie concrètement qu'une exploitation de caméras de surveillance dans des vestiaires ou toilettes n'est pas conforme aux exigences de la protection des données.

Nous avons dû faire face à un nombre croissant de demandes et de reportages dans la presse qui se réfèrent à la vidéosurveillance dans les toilettes et/ou vestiaires de piscines ainsi que dans les salles de fitness et les restaurants. En automne, ce sujet a également fait la une des journaux: plusieurs piscines surveillaient leurs vestiaires à l'aide de caméras vidéo pour tenter de prévenir les vols. Suite à des demandes de citoyens, nous avons procédé à un examen des faits dans une de ces piscines en inspectant de plus près l'installation vidéosurveillance se trouvant dans ses vestiaires.

Nous avons pu constater que les caméras n'enregistraient pas dans les cabines du vestiaire, mais dans l'espace commun de celui-ci, près des casiers, étant donné que de nombreux cambriolages ou vols avaient été recensés à cet endroit. De surcroît, la mauvaise visibilité sur l'ensemble de l'installation aggrave le problème. Vu la disposition du vestiaire (en particulier les locaux séparés par sexe et les bancs placés devant les casiers), beaucoup d'usagers de la piscine n'utilisent pas les cabines, mais se changent directement devant les casiers surveillés par les caméras. Cela signifie qu'une grande partie des usagers qui se changent se trouvent dans le champ de vision des caméras vidéo. Les personnes concernées n'en étaient en majorité pas conscientes, car aucune indication spéciale ne rendait attentif à la présence de caméras de surveillance. Cela signifie que dans ce cas

concret la vidéosurveillance a le même effet que si elle est effectuée directement dans les cabines du vestiaire. Partant, porte atteinte à l'intimité des personnes concernées.

Pour éviter de telles situations, toute vidéosurveillance dans des vestiaires ou toilettes doit, outre les exigences d'ordre général (cf. notre feuillet thématique «Vidéosurveillance effectuée par des particuliers», à consulter sur notre site www.leprepose.ch sous Protection des données – Vidéosurveillance), remplir les conditions suivantes pour que l'exploitation soit conforme aux exigences de la protection des données: Les caméras vidéo ne doivent pas être installées dans les cabines de vestiaires ou dans les toilettes. Des caméras peuvent être installées dans les vestiaires mêmes ou dans l'espace devant les toilettes pour autant que leur champ de vision n'englobe pas toute la surface et que les personnes présentes aient la possibilité de se changer sans être filmées (p. ex. dans les cabines individuelles du vestiaire ou dans des recoins qui ne sont pas dans le champ de vision des caméras). Les cabines individuelles doivent être hors du champ de vision des caméras. Les possibilités de se changer sans être filmé doivent être suffisamment nombreuses pour que l'on puisse attendre des usagers qu'ils les utilisent. Des panneaux bien visibles doivent en outre indiquer clairement quels espaces sont surveillés et lesquels ne le sont pas.

Vous trouverez plus d'informations à ce sujet dans les explications que nous avons publiées sur notre site web www.leprepose.ch, sous Protection des données – Vidéosurveillance concernant la vidéosurveillance dans les vestiaires et toilettes.

Les exploitants de la piscine concernée ont pris au sérieux les soucis des usagers de même que nos objections contre la surveillance vidéo dans les vestiaires. Ils ont donc décidé d'élaborer un nouveau concept et renoncent pour le moment à surveiller les vestiaires. Lors d'une visite des lieux nous avons pu constater, que les caméras mises en cause ont immédiatement été retirées et que l'installation de surveillance de la piscine est maintenant conforme aux exigences de la protection des données.

1.2.2 Stockage centralisé de photos de clients dans les stations de ski

Le système de contrôle d'accès utilisé dans de nombreuses stations de ski suisses doit être amélioré du point de vue de la sécurité des données. Le fabricant du système a accepté de réaliser dans les meilleurs délais les améliorations techniques que nous avons requis.

Basé sur les résultats d'un contrôle que nous avons effectué antérieurement (cf. notre 18e rapport d'activités 2010/2011, ch. 1.2.5 ainsi que notre 19e rapport d'activités 2011/2012, ch. 1.2.9), le système de contrôle d'accès utilisé par de nombreuses stations de ski en Suisse doit faire l'objet d'améliorations au niveau de la sécurité des données. Ainsi, les photos des usagers sont stockées sur un serveur central dans un format qui n'est en principe lisible que par le logiciel propriétaire du système, une mesure qui devrait rendre plus difficile une utilisation abusive des photos. Cependant, comme cette base de données ne contient pas seulement des photos d'usagers, mais également des données personnelles sensibles, cette protection s'avère insuffisante.

Nous avons, en collaboration avec le fabricant du système, examiné comment améliorer la sécurité des données. Il s'est avéré qu'une adaptation immédiate des systèmes existants sur le plan technique ne peut être entreprise. Le fabricant du système s'est néanmoins engagé à concevoir aussi rapidement que possible des mesures appropriées et à les incorporer dans ses produits. Nous suivrons ce développement avec attention et vous en informerons en temps voulu.

1.2.3 Voyageurs sans titre de transport valable – contrôle de la base de données auprès des CFF

Nous avons procédé auprès des CFF à un contrôle portant sur le traitement des données relatives aux voyageurs sans titre de transport valable. A cette occasion, il a été constaté qu'une base légale au sens formel manque pour le système d'information proprement dit. L'Office fédéral des transports a de ce fait accepté d'entamer les démarches nécessaires sur le plan législatif. Lors de notre contrôle sur place, les CFF n'avaient pas encore mis en œuvre la suppression prévue des données dans leur système d'information. Nous sommes actuellement en train d'étudier le concept de suppression des données qui a été élaboré entretemps, ainsi que sa mise en œuvre.

Nous avons reçu plusieurs demandes concernant le traitement que les CFF effectuent avec les données des voyageurs sans titre de transport valable. Diverses

informations sont apparues dans la presse à ce sujet. Le nombre de personnes concernées par ce traitement est considérable étant donné que les CFF recensent également les voyageurs qui ont oublié d'emporter leur abonnement. Nous avons par voie de conséquence procédé à un contrôle auprès des CFF.

Les données des voyageurs sans titre de transport valable sont traitées dans le système d'information RogF des CFF. Ce système se base sur la loi fédérale sur le transport de voyageurs (LTV) ainsi que sur les dispositions tarifaires des entreprises de transport suisses. Le «Tarif 600» contient les conditions générales pour le transport des voyageurs, le «Tarif 600.5» les lignes directrices pour le traitement des voyageurs sans titre de transport valable. Ce dernier s'appuie principalement sur la loi fédérale sur le transport de voyageurs qui prévoit que les personnes qui ne peuvent pas présenter de titre de transport valable doivent payer un supplément. Ce supplément peut être majoré dans les cas où le voyageur récidive. Les CFF disposent d'autre part d'une directive du groupe relative à la protection des données. Ces derniers ont pu nous expliquer quelles données sont traitées et à quelles fins elles le sont dans le système RogF, toutefois les détails de ces traitements (finalités, catégories de données, accès aux données, suppression des données, etc.) ne sont décrits nulle part, ni dans la documentation des CFF, ni dans une base légale.

Selon les indications des CFF, le traitement des données a lieu comme suit: l'agent d'accompagnement du train effectue ses contrôles à l'aide de son terminal mobile pour le personnel roulant. Ce terminal mobile ne dispose pas de liaison en ligne avec le système RogF. Cela signifie que les données concernant les voyageurs sans titre de transport valable, qui ont été saisies sur le terminal mobile, ne sont transférées dans la base de données RogF qu'après le service. Si l'agent d'accompagnement de train a affaire à un passager ne possédant pas de titre de transport valable, il remplit en plus le formulaire 7000, qui sert de titre de transport et est en outre sauvegardé par les CFF. Ce formulaire est rempli dans les cas où un voyageur a oublié son abonnement personnel (p.ex. un AG) et ne peut pas prouver son identité ou s'il possède un titre de transport, mais a oublié son abonnement demi-tarif. Dans ces deux cas, la personne concernée dispose de dix jours pour présenter l'abonnement qu'elle avait oublié, après quoi l'affaire est classée.

Dans le cadre de la concession qui leur a été attribuée, et selon la définition de la loi sur la protection des données les CFF agissent en tant qu'organe fédéral. Ils doivent donc disposer d'une base légale pour traiter des données personnelles. Cette base légale doit être de nature formelle (p. ex. une loi fédérale adoptée par le parlement) dans les cas où le traitement concerne des données personnelles sensibles. La LTV réglemente la perception des suppléments, mais pas le système

d'information en soi. Parallèlement, la loi sur la protection des données stipule que des données personnelles sensibles peuvent être traitées sans base légale dans les cas où cela est exceptionnellement nécessaire pour une tâche clairement définie dans la loi au sens formel. Nous avons conclu que les CFF doivent exploiter un système d'information afin de remplir leur devoir légal, notamment la majoration du supplément pour les personnes récidivistes. Un tel traitement ne peut cependant s'appuyer sur la loi sur la protection des données que dans des cas exceptionnels. Le cas présent ne constitue pas une telle exception.

Vu la définition claire de la tâche légale dans la LTV, nous avons néanmoins pu renoncer à interdire le système d'information RogF jusqu'à l'élaboration de la base légale nécessaire. La base actuelle reste cependant lacunaire, raison pour laquelle le système pourra continuer à être exploité pour une période restreinte uniquement. La base légale manquante doit être créée aussi vite que possible. La difficulté à laquelle nous avons été confronté dans ce cas est de ne pas pouvoir exiger cette base de la part des CFF, du fait qu'ils ne peuvent pas eux-mêmes mettre en route un processus législatif. Ils peuvent cependant intervenir auprès de l'Office fédéral des transports (OFT) pour que celui-ci lance le processus. C'est pour cette raison que nous avons proposé aux CFF de nous communiquer, en coordination avec l'OFT, si les démarches nécessaires à la création d'une base légale pour l'exploitation de tels systèmes ont été entreprises. En même temps, nous nous sommes réservés le droit de recommander aux CFF de renoncer aux traitements de données dans le système RogF au cas où ces démarches n'étaient pas mises en œuvre. Nous avons également proposé aux CFF de définir le détail des traitements de données effectués dans des instructions ou directives en attendant que les bases légales voient le jour.

A l'origine, les CFF avaient prévu de supprimer les données stockées dans RogF au bout de deux ans. Notre contrôle sur place a cependant révélé qu'aucune donnée n'avait jusqu'ici été supprimée. Ainsi, le système contient encore des données datant des années 1999 et 2000. Un stockage de données pour une telle durée viole le principe de la proportionnalité. Lors de notre contrôle, les CFF étaient en train d'élaborer un concept pour la suppression des données. Ce concept doit préciser quelles données sont conservées, pendant combien de temps, pour quelle finalité et comment la suppression des données sera effectuée. Nous avons recommandé aux CFF d'élaborer ce concept d'ici la fin de 2012, de nous le soumettre et en même temps de procéder à la suppression des données qui ne sont plus nécessaires. Les formulaires 7000 sauvegardés n'avaient également pas été supprimés au moment de notre contrôle. Effectivement, des documents qui dataient déjà de l'année 2006 ont été retrouvés. Nous avons de ce fait émis une recommandation de procéder

de la même manière que pour la suppression des données dans RogF. D'autres recommandations concernaient l'élaboration d'un règlement de traitement pour le système ainsi que pour la génération de mots de passe.

Les CFF ont accepté nos propositions et recommandations. L'OFT de son côté nous a assuré qu'il entreprendrait les démarches nécessaires à la création des bases légales manquantes. Le concept pour la suppression des données ainsi que le règlement de traitement nous ont d'ores et déjà été délivrés. Ces documents feront l'objet d'une analyse de notre part par le biais de laquelle nous vérifierons si les données ont effectivement été supprimées. Parallèlement, nous continuerons à suivre les démarches sur le plan législatif.

1.2.4 Dispositions d'exécution concernant la législation dans le domaine du sport

Le 17 juin 2011, le Parlement a adopté une nouvelle loi sur les systèmes d'information de la Confédération dans le domaine du sport, en même temps que la loi fédérale sur l'encouragement du sport et de l'activité physique. Ces dispositions entrées en vigueur le 1er octobre 2012 ont permis de créer les bases légales pour la lutte antidopage en Suisse. Nous nous sommes prononcés sur les dispositions d'exécution requises. Nos objections concernant la durée de conservation de données personnelles ont été prises en compte.

L'ordonnance relative à la loi sur les systèmes d'information de la Confédération dans le domaine du sport règle entre autres le traitement des données personnelles. Dans le cadre de la consultation des offices, nous nous sommes exprimés en particulier sur la durée de conservation des données. La durée se détermine par rapport au principe de la proportionnalité: en effet, les données doivent être conservées uniquement aussi longtemps que le but de leur traitement le requiert. Nos remarques ont été prises en compte en ce sens que la durée de leur sauvegarde a été définie différemment en fonction du genre de données et du but du traitement. Ainsi, à l'expiration des délais, les données sont soit archivées et effacées du système, soit anonymisées.

L'entrée en vigueur de la loi fédérale sur l'encouragement du sport et de l'activité physique (LESp) a créé une base légale pour la lutte antidopage en Suisse. Jusqu'ici, les mesures de répression dans ce domaine reposait sur le consentement des athlètes à effectuer les contrôles nécessaires. Toutefois, ce consentement donné n'était pas libre, car en cas de refus, il n'y avait aucune autre solution valable. En

effet, si au lieu du consentement au traitement des données, la seule solution est de renoncer à la compétition sportive envisagée, on ne peut pas parler d'une alternative de valeur égale. De ce fait, les déclarations en question ne pouvaient être considérées comme des consentements au sens juridique du terme. Grâce à la base légale que nous avons suggérée, les sportifs qui participent régulièrement à des compétitions peuvent être soumis en tout temps à des contrôles de dopage, qu'ils aient ou non donné leur consentement (cf. notre 15e rapport d'activités 2007/2008, ch. 1.5.3).

En outre, l'entrée en vigueur de la LESp fournit les bases légales permettant d'assurer l'échange de données nécessaires avec les laboratoires antidopage suisses et internationaux. Néanmoins, étant donné que des informations sensibles peuvent être concernées, elles ne peuvent être transmises sans réserve à des laboratoires antidopage internationaux. Le service qui envoie les données ne doit transmettre aucune donnée qui impliquerait une violation des droits de la personnalité, notamment si l'organisme destinataire ne peut garantir une protection des données suffisante. La protection est réputée suffisante lorsque le pays destinataire dispose d'un niveau suffisant de protection des données ou si une réglementation contractuelle est prévue. (cf. ch. 1.2.6 du présent rapport d'activités).

1.2.5 Traitement de données personnelles en relation avec des manifestations sportives

Au cours de l'exercice écoulé, nous avons clos l'examen des faits auprès d'un fournisseur de services dans le domaine des manifestations sportives sans avoir besoin d'établir de recommandation. Toutefois, l'information sur le traitement des données effectué par l'organisateur est insuffisante. En outre, le consentement au traitement des données souffre du manque de certaines conditions au niveau juridique.

Nous avons pu clore l'examen des faits sur le fournisseur de services sans recommandation. En effet, le fournisseur de services a mis en œuvre nos propositions d'amélioration dans son système (cf. notre 19e rapport d'activités 2011/2012, ch. 1.2.10).

Toutefois, force a été de constater que pour les personnes concernées, les traitements de données effectués par les organisateurs présentaient encore des lacunes au niveau de l'information et de la validité du consentement. La publication de listes de départ et de listes de classement sur internet n'est pas nécessaire

à l'organisation d'une manifestation sportive. Pour cette raison, les participants doivent se voir offrir la possibilité d'un droit dit d'opting-out (droit de retrait). La formulation choisie par plusieurs organisateurs dans leurs règlements ou dans leurs déclarations de protection de données, à savoir «Le présent consentement est la condition à la participation», ne répond pas aux prescriptions de la loi sur la protection des données. Comme dans d'autres domaines, le consentement n'est pas donné librement lorsqu'en cas de refus, il n'y a aucune autre solution d'égale valeur, d'autant plus que le traitement des données n'est pas nécessaire au but poursuivi. Les associations sportives et les organisateurs de rencontres ont été enjoints de mettre en œuvre un traitement des données uniforme conforme aux dispositions légales en la matière.

1.2.6 Lutte contre le dopage et communication de données personnelles à l'étranger

Depuis l'entrée en vigueur de la loi fédérale sur l'encouragement du sport et de l'activité physique, une base légale existe pour la communication de données à l'Agence mondiale d'antidopage. Etant donné qu'il s'agit d'une communication de données à l'étranger, il est nécessaire de garantir un niveau de protection des données suffisant par des dispositions contractuelles.

La nouvelle loi fédérale sur l'encouragement du sport et de l'activité physique (LESp) règle sous le titre «Mesures de lutte contre le dopage», la saisie, le traitement et l'échange de données personnelles dans le cadre de la lutte contre le dopage. Nous avons été contactés par des associations sportives qui voulaient savoir si cette nouvelle loi permettait sans autre de transmettre des données médicales de sportifs au serveur de l'Agence Mondiale Antidopage (AMA) situé à Montréal. Le PFPDT a analysé les faits et pris position.

Sous l'ancien droit, la transmission de données de sportifs vers le serveur de l'AMA à Montréal se heurtait à deux difficultés: d'une part, il n'existait aucune base légale justifiant la saisie, le traitement et l'échange de données personnelles dans le cadre de la lutte contre le dopage. On se basait donc sur le consentement des sportifs. Etant donné que les consentements n'étaient pas délivrés de plein gré, du point de vue de la protection des données, leur validité était fortement remise en question (cf. notre 15e rapport d'activités 2007/2008, ch. 1.5.4 et notre 17e rapport d'activités 2009/2010, ch. 1.2.7). D'autre part, comme l'AMA n'exerce pas une activité commerciale, mais idéologique, elle n'est ni soumise à la législation sur la protection des données canadienne, ni à celle de la province du Québec. Cela

signifie qu'il n'existe pas de niveau de protection des données suffisant pour les livraisons de données à l'AMA à Montréal et donc que celles-ci ne peuvent être autorisées selon l'article 6 LPD que si le niveau de protection des données est assuré d'une autre manière, p. ex. par une disposition contractuelle (cf. notre 15e rapport d'activités 2007/2008, ch. 1.5.3).

La nouvelle LESp offre une solution au premier problème. Aussi bien la saisie que le traitement de données personnelles pour la lutte contre le dopage que l'échange de ces données avec des organes nationaux ou internationaux de lutte contre le dopage font maintenant l'objet d'une réglementation légale et ne nécessitent donc plus le consentement des personnes concernées (cf. ch. 1.2.4 du présent rapport d'activités). Ceci facilite non seulement le travail des organes de lutte contre le dopage, mais permet également aux sportifs d'y voir plus clair en ce qui concerne leurs droits et obligations lors de contrôles anti-dopage.

Par contre, la nouvelle loi n'a pas simplifié l'exigence visant à assurer qu'un niveau de protection des données adéquat existe dans l'Etat destinataire lors des livraisons de données. Au contraire, l'article 25 alinéa 4 LESp dit clairement qu'une communication des données doit être refusée lorsque le destinataire n'assure pas un niveau de protection des données adéquat. Cette disposition réitère ainsi la règle générale de la loi fédérale sur la protection des données et précise que même la lutte justifiée contre le dopage ne doit pas mener à une situation mettant en danger la protection de la personnalité des personnes concernées.

Nous avons informé les associations qui nous ont contactées que, même avec la nouvelle LESp, le niveau de protection des données devait être assuré par des dispositions contractuelles et que des accords avec l'AMA dans ce sens devaient donc être conclus, respectivement maintenus.

1.2.7 Tour d'horizon des technologies biométriques

Dans le cadre des projets techniques initiés régulièrement, nous avons procédé à un tour d'horizon des technologies biométriques actuelles. Nous nous sommes basés sur notre expérience de veille technologique régulière pour maintenir une vision actuelle de ce domaine en continuel développement. Le test de différents produits a permis de compléter ce projet par une partie plus pratique.

Nos activités de contrôle et de conseil nous confrontent régulièrement à des questions liées aux technologies biométriques qui connaissent un succès grandissant. Face à ces développements constants, nous avons initié une étude

interne qui a permis de faire un tour d'horizon des différentes technologies connues et utilisées à ce jour, tant au niveau de la recherche que de la pratique.

Nous avons également testé de manière pratique différents systèmes de reconnaissance grâce à l'acquisition ou à la mise à disposition de plusieurs lecteurs d'empreintes biométriques. Notre approche dans cette étude s'est focalisée principalement sur le respect de la sphère privée offert par les différentes technologies existantes et la traçabilité des différentes caractéristiques biométriques. Les technologies les plus adaptées sont ainsi celles qui présentent le moins de risques au niveau de la protection des données personnelles et qui laissent également un minimum de traces. Nous avons conclu cette étude en constatant qu'il existe aujourd'hui des technologies biométriques, telles que la reconnaissance du système veineux ou la reconnaissance de la frappe sur le clavier, qui sont respectueuses de la vie privée mais également faciles d'utilisation.

1.2.8 Formation concernant l'élaboration d'un règlement de traitement

Nous avons élaboré un règlement de traitement en collaboration avec le conseiller en matière de protection des données du Département fédéral de la défense, de la protection de la population et des sports (DDPS). L'objectif était de montrer comment procéder et quel effort doit être mis en œuvre pour obtenir la transparence nécessaire. Sur la base des expériences faites, nous avons formé les autres conseillers en matière de protection des données des divers offices du DDPS.

Le délégué à la protection des données du DDPS nous a demandé de donner dans son département une formation sur l'élaboration d'un règlement de traitement. Nous avons accepté puis avons, avant la formation, créé ensemble avec le délégué à la protection des données et le maître de fichier un règlement de traitement pour une application concrète. Les discussions ont déjà commencé au moment de traiter la première question, qui porte sur le but ou la finalité de l'application. Ce point répond à la question de savoir ce que l'on veut obtenir avec l'application et pourquoi. Souvent, ces descriptions mentionnent plutôt les tâches ou fonctions qui doivent être remplies par l'application, alors que les tâches ou fonctions devraient plutôt s'aligner avec le but visé.

L'examen du système et de son contexte (documentation des unités organisationnelles affectées par le système ou l'application) consistait à comprendre l'application dans ses grandes lignes. Quelles données sont traitées

dans quelles unités organisationnelles, pourquoi et dans quel but? Pourquoi (dans quel but) les données personnelles sont-elles transmises à d'autres organes? Cette transmission de données est-elle aussi judicieuse du point de vue de la protection des données ou pourrait-on éventuellement exécuter les tâches avec des données anonymes ou pseudonymisées?

Après que l'analyse ci-dessus nous ait procuré une vue d'ensemble de l'application, nous avons commencé à documenter les processus qui devaient décrire plus en détail comment les tâches seraient exécutées au sein des unités organisationnelles. Le conseiller en matière de protection des données analyse les processus principalement dans l'optique des personnes concernées. Cette optique diffère de celle du maître de fichier qui lui met l'accent plutôt sur l'efficacité du traitement des données. L'organisation de projet comprend la plupart du temps des représentants des utilisateurs et du service informatique ainsi que le chef de projet, mais généralement pas de conseiller en matière de protection des données. Le donneur d'ordre du projet ferait bien, notamment pour les projets sensibles, d'impliquer également le conseiller en matière de protection des données de l'organisation de projet concernée pour éviter le risque que les aspects de la protection des données ne soient pas suffisamment pris en compte. Cette négligence peut par la suite entraîner de sérieux inconvénients.

Pour que le conseiller en matière de protection des données sache ce qui se fait du point de vue de l'application et qu'il puisse participer activement, il doit être tenu informé des nouveaux projets ou des modifications aux systèmes existants (applications). L'analyse d'une application existante a montré, entre autres, combien il est souvent difficile de comprendre les aspects techniques et organisationnels d'un système. D'autre part, l'élaboration de ce règlement de traitement a également montré que des réglementations judicieuses et définitives ne sont possibles que si la transparence nécessaire existe.

1.3 Internet et télécommunication

1.3.1 Explications concernant les mises au pilori sur internet

La mise au pilori sur internet est une pratique qui fait de plus en plus d'adeptes. Les clients qui ne paient pas leurs factures, les membres d'autorités qui prennent des décisions incommodantes ou les personnes défendant une certaine opinion politique sont inscrits dans une liste publiée sur internet. Ils sont de ce fait exposés publiquement à des reproches. De telles mises au pilori sur internet violent les droits de la personnalité des personnes concernées et sont donc contraires à la loi.

Une mise au pilori sur internet pose problème du point de vue de la protection de la personnalité: les personnes qui n'ont pas agi ou décidé dans le sens de l'auteur de la liste sont ainsi répertoriées sur internet et couvertes de reproches provocateurs. Le pilori est accessible dans le monde entier 24 heures sur 24 et les informations qui y ont été publiées peuvent encore être consultées pendant de nombreuses années. Comme ces informations n'ont pas été élaborées avec le soin journalistique requis et ne reflètent pas de façon nuancée les événements contestés, ces publications ne répondent pas à un besoin d'information général. Ces mises au pilori ont pour objectif de montrer du doigt et de dénigrer les personnes mentionnées. Ceci peut avoir des conséquences graves. Le PFPDT précise qu'il n'existe pas de motifs qui permettent de justifier une telle atteinte à la personnalité.

Contrairement à ce que l'on croit couramment, les personnes concernées peuvent être atteintes dans leur personnalité même dans les cas où les données publiées sur leur compte sont déjà connues. Ceci peut être dû au fait que ces données sont mises en relation avec d'autres et publiées dans un contexte complètement différent, qui n'a en fait plus rien à voir avec la publication d'origine. Même dans ces cas l'utilisation des données en question dans le nouveau but, à savoir la mise au pilori sur internet n'est pas justifiée.

Il en va de même des mises au pilori de membres d'autorité, c'est-à-dire des listes noires de membres d'autorités qui ont soi-disant eu un comportement fautif. Elles doivent être traitées avec la plus grande prudence. Il est évidemment permis de critiquer des personnes qui exercent une fonction publique, mais seulement aussi longtemps que cette critique reste objective et qu'elle se réfère à l'activité du membre de l'autorité, une condition qui n'est en règle générale pas remplie lors des

mises au pilori sur internet, étant donné qu'une description sommaire et partiale des faits ne peut en règle générale pas être qualifiée d'objective. Les publications ne peuvent en aucun cas contenir des informations à caractère personnel telles que l'adresse privée, le numéro de téléphone, l'adresse de courriel, des photos non encore publiées, etc. Les commentaires diffamants ou même des exhortations à contacter la personne en dehors de son activité publique ne peuvent être publiés.

Vous trouverez de plus amples informations concernant la mise au pilori sur Internet sur notre site www.leprepose.ch, sous Protection des données – Internet et ordinateur.

1.3.2 Prises de vue des voies publiques sur Internet – Arrêt du Tribunal fédéral

Le 31 mai 2012, le Tribunal fédéral a rendu un arrêt sur les aspects touchant à la protection des données dans l'affaire Google Street View. Les points essentiels en sont l'applicabilité de la loi suisse sur la protection des données, les exigences posées à l'utilisation d'un procédé automatique d'anonymisation, l'anonymisation des établissements sensibles et les prises de vue des domaines privés qui ne sont pas visibles pour les passants.

Dans son arrêt (ATF 138 II 346), le Tribunal fédéral s'est tout d'abord prononcé sur la compétence des autorités et tribunaux suisses quant à l'appréciation de l'état de fait. Un traitement de données est soumis au droit suisse de la protection des données et relève de notre compétence dès lors qu'un lien suffisant avec la Suisse existe – ce qui est également le cas lorsque les serveurs sont stationnés à l'étranger. Dans l'affaire Google Street View, des informations sur des personnes, des rues et des places en Suisse sont rassemblées et publiées, donc consultables sur internet depuis la Suisse. Cet arrêt est important en ce sens qu'il précise que la loi suisse sur la protection des données est également applicable à un traitement qui a lieu en partie à l'étranger lorsqu'un lien suffisant avec la Suisse existe.

L'un des points majeurs de l'ensemble de la procédure était de savoir si Google devait flouter totalement les visages et les numéros de plaques dans les prises de vue du service Street View avant la mise en ligne. Le Tribunal fédéral a accordé une tolérance d'erreur d'1% dans l'anonymisation automatique. Toutefois, cinq conditions doivent être remplies:

- L'objectif est d'atteindre une anonymisation totale par tous les moyens techniques disponibles et l'anonymisation automatique doit être en permanence adaptée aux progrès technologiques.

- Un lien bien visible doit être à la disposition des utilisateurs, par exemple avec la mention claire «Demander l'anonymisation»; il leur permettra de requérir une anonymisation suffisante des contenus illicites.
- Les personnes et les véhicules situés à proximité des établissements sensibles comme les centres d'accueil pour femmes battues, les maisons de retraite, les prisons, les écoles, les tribunaux et les hôpitaux doivent être complètement anonymisées avant leur mise en ligne. Cela de telle manière qu'en plus des visages, d'autres caractéristiques individuelles comme la couleur de la peau, les vêtements, les moyens auxiliaires pour handicapés etc. ne soient plus identifiables.
- Les espaces privés (comme les cours et les jardins clos) doivent être respectés. Les prises de vue faites à partir d'une hauteur de deux mètres et qu'un passant normal ne peut voir ne peuvent pas être publiés sur Street View. Si la personne concernée n'a pas donné son consentement, les prises de vue déjà publiées de ce type d'espaces privés doivent être retirées.
- Lorsque de nouvelles prises de vue doivent être effectuées ou être mises en ligne, il faut d'une part le publier dans les médias et indiquer clairement en ligne les droits d'opposition.

Nous sommes en contact avec Google quant à la mise en œuvre des conditions imposées par le Tribunal fédéral et en contrôleront le respect de manière suivie.

1.3.3 Echange de contenus sur internet – situation juridique après l'arrêt Logistep

Après l'arrêt du Tribunal fédéral en la cause Logistep, une certaine incertitude existe en ce qui concerne la poursuite des violations des droits d'auteur. Est-elle encore possible selon la législation actuelle? Des efforts sont en cours en vue de créer des bases légales permettant de prendre des mesures facilitant le respect des droits d'auteur sur internet et ainsi d'apporter un peu plus de clarté dans cette affaire.

L'arrêt dans l'affaire Logistep (cf. notre 18e rapport d'activités 2010/2011, ch. 1.3.5) a provoqué la confusion en ce qui concerne la portée de cette décision sur la poursuite de violations des droits d'auteur sur internet. Les procureurs interprètent l'arrêt dans ce sens que toute collecte d'adresses IP sur internet dans le but de poursuivre des violations de droits d'auteur est contraire à la loi et que les preuves

récoltées sur cette base sont illicites. Le PFPDT est toutefois d'avis que la collecte et le traitement de telles données personnelles continuent à être possibles pour autant que les principes suivants soient respectés (cf. notre 19e rapport d'activités 2011/2012, ch. 1.3.7):

- il doit être assuré que la collecte et l'enregistrement des données ne va pas au-delà de ce qui est absolument nécessaire pour déposer une plainte pénale contre des personnes présumées avoir violé les droits d'auteur;
- il doit être assuré que les négociations pour les prétentions en réparation du dommage menées entre les détenteurs des droits d'auteur et les personnes présumées avoir violé ces droits n'ont lieu qu'à leur initiative ou alors après une condamnation pénale;
- les détenteurs de droits d'auteur doivent rendre la collecte de données personnelles et le but de leur traitement aussi visibles que possible pour les personnes concernées, notamment en révélant en toute transparence leur manière de procéder à un endroit facilement repérable et accessible sur leur site web (en particulier des indications détaillées sur la nature et l'étendue des données collectées); ils doivent exprimer clairement que des actions en réparation du dommage ne seront engagées qu'envers des personnes condamnées pénalement pour violation des droits d'auteur.

La preuve qu'une telle collecte de données est conforme à la législation actuelle pourrait être apportée par les détenteurs des droits d'auteur en demandant à un tribunal de dernière instance de définir clairement les exigences d'une administration des preuves conforme à la loi sur la protection des données dans un cas de violation des droits d'auteur sur internet.

Nous nous sommes référés à plusieurs reprises au rapport de gestion 2010 du Tribunal fédéral qui, dans ses rares «Indications à l'intention du législateur», signale les dispositions légales jugées insuffisantes dans le domaine de la protection des droits d'auteur. C'est surtout notre intervention dans le cadre d'un postulat parlementaire qui a finalement fait évoluer les choses dans ce domaine. Un groupe de travail mandaté par Madame la Conseillère fédérale Sommaruga examinera d'ici la fin de 2013 les possibilités d'adapter le droit d'auteur à l'évolution de la technologie. Ce mandat inclut l'examen de mesures permettant de faire appliquer plus facilement le droit sur internet.

1.3.4 Plateforme immobilière sur Internet

Nous avons examiné, du point de vue de la protection des données, un site internet sur lequel de futurs locataires peuvent constituer un dossier électronique de postulation pour un appartement.

Deux entreprises nous ont présenté leur projet d'élargissement de leur site immobilier et nous ont demandé de l'examiner sous l'angle de la protection des données. Ce site a pour but de donner aux éventuels locataires la possibilité de constituer leur dossier en ligne sur un modèle structuré. Dans ce contexte, l'un des deux partenaires livre à cet effet sur demande du locataire une estimation de la solvabilité ou des extraits du registre des poursuites. Ils ont mis au point ce site en tenant compte des directives publiées sur notre site internet. Le locataire doit être informé de manière transparente des traitements de données qui le concernent et garder la maîtrise de ses données. Les deux entrepreneurs ne peuvent consulter le dossier. Le futur locataire seul décide à quelle régie immobilière le dossier doit être transmis. Nous avons constaté que le projet correspondait aux exigences essentielles de la protection des données et avons suggéré quelques autres propositions d'amélioration.

1.3.5 Monitoring des réseaux sociaux et protection des données

Entreprises et autorités sont de plus en plus nombreuses à vouloir apprendre ce que l'on dit d'elles dans les réseaux sociaux. Ce phénomène a donné naissance au monitoring.

En comparaison avec les médias traditionnels (journaux, stations de radio, chaînes de télévision), les médias sociaux comme Facebook, Google+, XING, Twitter ou les blogs ont acquis une importance grandissante ces derniers temps auprès des entreprises, autorités et autres organisations qui d'une part désirent savoir ce qui se dit d'elles dans les réseaux sociaux et de l'autre entendent y réagir de manière adéquate. Afin de permettre aux entreprises souhaitant obtenir rapidement une vue d'ensemble des informations qui les concernent sur les réseaux sociaux, certains prestataires de services ont mis sur le marché des programmes permettant de parcourir ces sites. On parle en l'occurrence de «Social Media Monitoring».

L'observation des réseaux sociaux ne saurait cependant être appliqué au mépris des principes régissant la protection des données: le suivi de certaines personnes physiques ou morales identifiées ou identifiables (monitoring) équivaut à un traitement de données au sens de la loi sur la protection des données. Les données

traitées peuvent concerner le contenu des messages publiés ou leurs auteurs. Certes, ces derniers publient volontairement leurs opinions ou leurs contributions à des débats sur les plateformes de médias sociaux. Or, le but initial du traitement des données n'inclut pas obligatoirement un monitoring. Autrement dit, la loi ne s'applique pas automatiquement à tout traitement de données techniquement possible. Enfin, aux termes de la loi sur la protection des données, des données publiées ne peuvent être utilisées à d'autres fins que celles prévues initialement.

Le PFPDT recommande notamment, lors d'un monitoring des réseaux sociaux, de se limiter au minimum nécessaire au but poursuivi par l'analyse. Les résultats du monitoring ne doivent pas permettre de faire de lien avec une personne. En outre, les usagers des plateformes de réseaux sociaux doivent être informés que de tels outils sont utilisés.

Pour plus d'informations à ce sujet, consulter notre site www.leprepose.ch sous Protection des données – Internet – Services en ligne.

1.3.6 Utilisation d'outils d'analyses de l'audience internet pour les organes de la Confédération

L'exploitant d'un site internet désirerait analyser les accès des utilisateurs afin d'apprendre quels sont leurs mouvements sur ce site ou afin d'améliorer son offre en ligne. L'utilisation de ce type d'outils peut toutefois avoir des aspects particulièrement perfides pour les sites internet de la Confédération.

Les outils d'analyse de l'audience internet offrent des fonctions typiques comme l'enregistrement de l'origine géographique des visiteurs, la durée de la consultation du site et les notions introduites dans le moteur de recherche sémantique. A l'aide d'un élément d'image spécial ainsi que d'un script, l'outil d'analyse est intégré sur la page Internet de l'exploitant. Si aucune mesure spécifique n'est prise, ce type de service peut saisir les accès sur le site internet, car lorsque l'utilisateur appelle l'élément d'image, son adresse IP est enregistrée par ses serveurs. Etant donné que les adresses IP doivent être considérées comme des données personnelles, la loi sur la protection des données (LPD) est applicable.

À l'aide d'un programme d'analyse, il est possible de répertorier et analyser des profils détaillés des utilisateurs, jusqu'à leurs activités sur le site. Ces profils d'utilisateurs peuvent constituer des profils de la personnalité au sens de la LPD. Or, les organes de la Confédération sont tenus de ne traiter des données personnelles que si ce traitement repose sur une base légale; dans le cas de

données personnelles sensibles et de profils de la personnalité, cette base légale doit être une loi au sens formel.

Au cours de l'analyse des accès sur le site internet, les données dites secondaires de l'internaute sont transmises au fournisseur de l'outil d'analyse. Le traitement des données par cette catégorie de fournisseurs est à qualifier de traitement de données par des tiers, lequel nécessite aussi une base légale.

Si le serveur du fournisseur de l'outil d'analyse se trouve à l'étranger, il faut en outre respecter les règles concernant le transfert transfrontalier de données. Le transfert de données personnelles à l'étranger risque de donner aux autorités du pays en question la possibilité d'accéder à ces données en s'appuyant sur ses lois nationales. Il s'agit là d'un point particulièrement délicat pour les organes de la Confédération, car il leur incombe le devoir de traiter les données personnelles des citoyens avec précaution et de les protéger, notamment contre un accès indu d'autorités étrangères.

Il est donc recommandé aux autorités fédérales, essentiellement pour ce dernier motif, de renoncer à utiliser ce type d'outils et de rechercher d'autres variantes. Par contre, si des mesures spéciales sont à même de garantir que l'analyse ne permettra pas de relever des données personnelles, la LPD n'est pas applicable. Une autre possibilité s'offre toutefois, à savoir que les statistiques d'audience sur internet soient effectuées sur la base de programmes installés directement sur le serveur de l'organe de la Confédération. Cette solution permet de garantir qu'aucune donnée personnelle ne sera communiquée à un tiers en dehors de l'administration fédérale.

1.3.7 Révision de la loi sur les publications officielles

La publication des textes officiels est régie par la loi sur les publications officielles. La révision de cette loi a pour but d'adapter le système aux dernières avancées technologiques et à l'évolution de la société. Nous nous sommes prononcés à son sujet au cours de la consultation des offices.

La loi sur les publications officielles règle la publication des recueils du droit fédéral et de la Feuille fédérale. Jusqu'ici, la loi prévoyait aussi la publication électronique, outre la version imprimée; seule la version imprimée était juridiquement valable. Or, la révision de la loi sur les publications officielles introduit un changement de régime et la version électronique serait également déterminante. Nous nous sommes prononcés sur cette révision dans le cadre de la consultation des

offices. Nous avons souligné à cette occasion que les publications officielles peuvent aussi renfermer des données personnelles sensibles, par exemple dans le cadre des notifications. Selon la loi sur la protection des données, un organe de la Confédération ne peut publier des données sensibles ou des profils de la personnalité que si une loi au sens formel le prévoit expressément. A notre demande, une base légale allant dans ce sens a été rajoutée dans la révision de la loi sur les publications officielles.

1.3.8 Révision de l'ordonnance GEVER

A l'avenir, les systèmes de gestion électronique des données de la Confédération devront être tenus uniquement sous forme électronique. L'ordonnance GEVER en constitue la base légale. Un certain potentiel de risque étant lié à ce changement, des mesures de sécurité doivent être prises. Nous nous sommes prononcés à ce propos quant aux aspects touchant la protection des données et avons communiqué notre prise de position dans le cadre de la consultation des offices.

Cette année encore, l'ordonnance GEVER a été l'objet de nos préoccupations. Elle repose sur un arrêté du Conseil fédéral selon lequel les départements et la Chancellerie fédérale doivent introduire des systèmes de gestion des affaires électroniques (systèmes GEVER). Le but étant que les documents de la Confédération soient, dans la mesure du possible, traités électroniquement. La base légale requise est créée par l'ordonnance GEVER qui repose sur la loi fédérale sur l'organisation du gouvernement et de l'administration.

Dans le cadre de la consultation des offices, nous nous sommes prononcés sur le remaniement de cette ordonnance GEVER. Les exigences relatives à la protection des documents, notamment par des mesures techniques et organisationnelles, en constitue un aspect central. Les unités de l'administration fédérale doivent élaborer un programme de sûreté de l'information conforme aux normes de sécurité requises. Les documents sensibles, pertinents, doivent être transmis et déposés sous forme chiffrée. Tous les documents traités dans un système GEVER doivent être traités de manière à éviter que des personnes non autorisées puissent les consulter. L'échange de données entre deux systèmes GEVER doit s'effectuer par un canal de transmission sécurisé. Les personnes qui disposent de droits d'accès étendus (tant du côté du fournisseur que du bénéficiaire des prestations) doivent être soumises au contrôle de sécurité des personnes. En outre, certaines actions effectuées dans le système GEVER sont consignées dans un journal. Cela

permet de suivre et de contrôler la licéité du traitement des données GEVER. Nos requêtes ont été prises en compte, ce qui a permis d'éliminer les différends au cours de la consultation des offices du point de vue de la protection des données.

1.4 Justice/Police/Sécurité

1.4.1 Mise en œuvre Schengen: évaluation de la protection des données dans les Etats baltes

Nous avons, en octobre 2012, participé pour la première fois à une évaluation Schengen dans le domaine de la protection des données. Une petite équipe d'experts a évalué les trois Etats baltes. Les expériences qui y ont été faites seront très utiles pour l'évaluation de la Suisse, qui devrait être effectuée prochainement.

C'est la première fois que nous avons participé à une évaluation Schengen dans le domaine de la protection des données. Le tour des trois Etats baltes Lituanie, Lettonie et Estonie était fixé du 14 au 20 octobre 2012. Ceux-ci avaient été évalués pour la première fois en 2006 et avaient alors fait l'objet de diverses recommandations. En règle générale, une nouvelle évaluation est effectuée tous les cinq ans. Dès que le programme d'évaluation est défini, on nomme les experts qui sont idéalement constitués de huit à dix personnes.

Chaque Etat membre peut déléguer un expert au maximum. Dans ce cas, le groupe d'expert procédant à l'évaluation était composée de six personnes. Préalablement à l'évaluation, les trois Etats concernés avaient dû prendre position sur les recommandations qui leur avaient été faites en répondant à des questions et livrer divers documents. Le contrôle sur place a été effectué auprès des autorités de protection des données ainsi qu'auprès des autorités policières. A cette occasion les experts ont eu la possibilité de poser des questions supplémentaires. C'est essentiellement pendant la durée de leur visite dans les Etats baltes que les experts ont échangé leurs opinions et rédigé les premiers jets de leurs rapports d'évaluation. Ceux-ci font 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». En même temps, ils ont émis des recommandations envers les Etats soumis à l'évaluation. Ces projets de rapports ont ensuite fait l'objet d'une consolidation entre les divers experts avant de consulter les Etats concernés. Ceci a été suivi par une mise au net des rapports entre les Etats évalués et les experts. Les rapports ont ensuite été présentés au groupe de travail du Conseil responsable des évaluations Schengen (SCHEVAL), où ils ont été discutés et adoptés. L'évaluation fait toujours l'objet d'un suivi au cours duquel les Etats concernés peuvent démontrer dans quelle mesure ils ont pu appliquer les recommandations.

En ce qui concerne la Suisse, elle a été évaluée en 2008. Les expériences que nous avons faites en l'espèce nous seront utiles pour la prochaine évaluation de la Suisse, qui devrait avoir lieu prochainement.

1.4.2 Mise en œuvre Schengen: signalements de personnes dans le SIS en vue de l'arrestation aux fins d'extradition

Dans le cadre du contrôle coordonné des signalements saisis dans le SIS conformément à la Convention d'application de l'Accord de Schengen (CAAS), nous avons reçu à notre questionnaire une réponse conjointe de l'Office fédéral de la police et de l'Office fédéral de la justice. Suite à cela, nous avons procédé à un contrôle sur place. Nous sommes arrivés à la conclusion que les traitements de données effectués en Suisse remplissent les conditions spécifiées dans l'article 95 CAAS. Le rapport final de l'Autorité de contrôle commune de Schengen concernant le contrôle coordonné n'a pas encore été publié.

L'Autorité de contrôle commune de Schengen (ACC) a décidé de soumettre à un contrôle les signalements de personnes qui ont été saisis dans le SIS en vue de leur arrestation à des fins d'extradition (art. 95 CAAS). Ces signalements équivalent à un mandat d'arrêt et dans la majorité des cas un mandat d'arrêt européen a été émis au préalable. L'ACC a élaboré un questionnaire qui a été transmis par les divers Etats membres, également par le PFPDT, aux autorités nationales compétentes. L'Office fédéral de la police (fedpol) ainsi que le domaine de direction Entraide judiciaire internationale de l'Office fédéral de la justice ont pris position ensemble sur ce questionnaire. L'ACC a ensuite demandé aux autorités de protection des données de tous les Etats Schengen de procéder à un contrôle sur place. Nous avons effectué ce contrôle le 5 juillet 2012 auprès de ladite direction de l'OFJ. Notre contrôle a surtout porté sur la procédure mise en place pour les signalements selon l'article 95 CAAS ainsi que sur la communication des données.

Après examen des réponses au questionnaire et sur la base du contrôle effectué sur place, nous avons conclu que les signalements soumis à examen remplissaient les exigences stipulées à l'article 95 CAAS. Nous avons transmis notre rapport à l'ACC qui rédigera un rapport final du contrôle coordonné. Ce dernier sera publié sur notre site web.

1.4.3 Mise en œuvre Schengen: information aux utilisateurs et mention légale lors des accès RIPOL, SIS et SYMIC

Dans le cadre du groupe de coordination Schengen des autorités suisses de protection des données, nous avons contacté l'Office fédéral de la police pour examiner les masques de requêtes et de résultats utilisées lors de recherche dans les systèmes RIPOL, SIS et SYMIC. Dans ce cadre-là, une analyse afin de déterminer si les informations liées aux banques de données consultées étaient suffisantes et si une mention d'avertissement légale devait y être incluse a été entreprise.

Le «groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre de l'accord d'association à Schengen» a relevé lors de sa séance du 10 mai 2012 qu'il était important que les utilisateurs des systèmes RIPOL, SIS et SYMIC soient conscients de quels systèmes proviennent les données qu'ils consultent lors de leurs recherches. Le groupe a également exprimé son inquiétude quant à la licéité des recherches effectuées par les utilisateurs et s'est interrogé sur la possibilité d'insérer une mention d'avertissement légale dans les masques de requête. Nous avons donc contacté l'Office fédéral de la police (fedpol) pour apporter des réponses aux questions du groupe de coordination.

Les informations fournies par fedpol accompagnées de captures d'écran illustrant les différents masques de résultats développés par celui-ci nous ont permis de constater que les informations sur les banques de données consultées par les utilisateurs sont disponibles sur les différents masques de façon très visible. De plus, il nous a été confirmé que les masques de requête sont développés directement par les fournisseurs de service des cantons tandis que les masques de résultats le sont par fedpol. Ainsi, si les cantons souhaitent introduire une mention d'avertissement légale directement sur les masques de requêtes, ils ont la possibilité de s'adresser à leurs fournisseurs de service. A notre demande, cette thématique a été traitée par l'autorité de contrôle commune Schengen (ACC) lors de sa séance du 4 octobre 2012. Les réactions de la majorité des Etats membres indiquent qu'aucune mention d'avertissement légale n'a été mise en place dans les différents systèmes utilisés. L'ACC ne juge donc pas opportun de recommander la mise en place de telles mentions légales. Par contre, l'ACC relève que, sur cette thématique, il faut avant tout favoriser et insister sur la formation des utilisateurs.

Ainsi, nous avons pu informer le groupe de coordination Schengen lors de la séance du 15 novembre 2012 des résultats de nos investigations. Nous avons conclu qu'il était important de mettre l'accent sur la formation des utilisateurs

des systèmes RIPOL, SIS et SYMIC pour répondre aux inquiétudes formulées par le groupe de coordination.

1.4.4 Accords avec les Etats-Unis pour le maintien de la Suisse dans le Visa Waiver Program

La signature avec les Etats-Unis de l'accord PCSC concernant l'échange de données ADN et dactyloscopiques et le mémorandum d'entente HSPD-6 réglant l'échange de données concernant des terroristes connus ou présumés permet à la Suisse de rester dans le programme américain d'exemption du visa (Visa Waiver Program). Des règles concernant la protection des données ont été introduites dans ces deux instruments.

L'accord PCSC (Cooperation in Preventing and Combating Serious Crime) prévoit l'échange de données dactyloscopiques et ADN dans le but de combattre la criminalité grave. L'échange se déroule en deux étapes. La première est une interrogation de la base de données de l'Etat requis afin de déterminer si le profil soumis y figure ou non (système «hit - no hit», concordance – non concordance). En cas de réponse positive («hit»), il est possible de passer à la seconde étape de la procédure, qui consiste à échanger des données personnelles et d'autres informations en lien avec le cas en question. La transmission de ces données est régie par le droit national de l'Etat requis. Les dispositions de l'accord PCSC relatives à la protection des données permettent de garantir les droits des personnes concernées. Les principes généraux de protection des données sont mentionnés clairement. Les données sensibles bénéficient d'une protection supplémentaire. Les particuliers peuvent faire valoir leurs droits (accès, rectification, blocage et effacement) en application des législations nationales. L'autorité de protection des données pourra également intervenir auprès de l'autorité de l'autre Etat.

Le mémorandum d'entente HSPD-6 (Homeland Security Presidential Directive 6) prévoit l'échange de données concernant des personnes ayant des relations au terrorisme. Cet instrument n'introduit aucun nouveau droit ni aucune nouvelle obligation. Le but de ce mémorandum d'entente est l'optimisation de la coopération existante sur la base du droit en vigueur. Il indique qu'en matière de protection des données les bases légales nationales sont applicables.

Nous avons apporté notre soutien à l'Office fédéral de la police (fedpol) en examinant les différents documents dans le cadre des négociations avec les autorités américaines. La signature de l'accord PCSC et du mémorandum d'entente HSPD-6 permet à la Suisse de rester dans le programme américain

d'exemption du visa (Visa Waiver Program) des Etats-Unis. Les Suissesses et les Suisses pourront continuer de se rendre aux Etats-Unis sans visa pour un séjour de courte durée (au maximum 90 jours). Des risques d'atteinte à la personnalité des personnes concernées, à savoir celles dont les données dactyloscopiques et les profils ADN sont traités, ne sont pas exclus. Il faut cependant noter que ces risques existent également dans la législation actuellement en vigueur et que les règles de protection des données contenues dans l'accord et le mémorandum d'entente HSPD-6 assurent une protection des droits des personnes concernées.

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

Dans le cadre de la consultation des offices, nous nous sommes prononcés sur le projet de révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Dorénavant, le recours à des programmes informatiques devrait reposer sur l'introduction d'une base légale. Nous avions aussi requis une base légale pour la communication de données dites de contenu en cas de prestations qui reposent sur des services de télécommunication.

Après avoir pris position, au cours des dernières années, à propos de divers projets législatifs concernant la surveillance de la correspondance par poste et télécommunication, nous avons récemment eu la possibilité de nous prononcer sur le dernier projet de révision totale de la loi fédérale. Nous estimons que la protection des données ne doit pas entraver l'efficacité de la lutte contre la criminalité. Toutefois, la surveillance de la correspondance par poste et télécommunication empiète sur un droit fondamental protégé par la constitution. Elle nécessite donc des bases légales formelles qui doivent en outre être formulées de manière suffisamment précise.

Nous nous sommes déjà prononcés sur l'absence de bases légales pour l'utilisation de programmes informatiques et autres chevaux de Troie (cf. notre 19e rapport d'activités 2011/2012, ch. 1.4.8). Le projet de loi qui nous a été présenté devrait fournir entres autres la disposition nécessaire à ce propos.

Nous avons aussi requis une base légale similaire pour la communication de données dites de contenu (par ex. les appareils de sauvegarde de données, les carnets d'adresses ou les documents établis par des utilisateurs) par des fournisseurs de services de communication dérivés comme les prestataires de services en nuage ou les fournisseurs d'espace de stockage. Nous estimons que

la communication de données de contenu sauvegardées sur internet doit être explicitement régie dans une loi au sens formel.

1.4.6 Loi sur le renseignement

Le projet de loi sur le renseignement dans sa version transmise en 2e procédure de consultation a été amélioré sur plusieurs points. Par contre, d'autres éléments sont toujours problématiques du point de vue de la protection des données, par exemple: certains moyens d'acquisition des informations et l'exclusion du Service de renseignement de la Confédération du champ d'application de la loi sur la transparence.

Le projet de loi sur le renseignement a fait l'objet de deux procédures de consultation des offices. Le projet de loi proposé en avril 2012 comportait plusieurs éléments très problématiques du point de vue de la protection des données. Les normes relatives aux différentes bases de données du Service de renseignement de la Confédération (SRC) étaient insuffisantes. Le projet prévoyait même un droit d'accès indirect encore plus défavorable aux personnes concernées que la réglementation en vigueur avant le 16 juillet 2012. Le projet soumis en consultation en octobre 2012 apporte des améliorations du point de vue de la protection des données. Les mesures d'acquisition des informations soumises à autorisation devront ainsi être approuvées par le Tribunal administratif fédéral et ces mesures concerneront un nombre limité de cas. Les dispositions relatives aux bases de données sont beaucoup plus détaillées que celles proposées dans le cadre de la première consultation. En ce qui concerne le droit d'accès, le nouveau projet prévoit un droit d'accès comparable à celui de la loi fédérale sur les systèmes d'information de police de la Confédération.

Cependant, plusieurs points du projet ne sont pas satisfaisants. Nous sommes d'avis que le SRC ne doit pas disposer de plus de moyens d'investigation que les autorités de poursuites pénales. Le projet doit donc être adapté en fonction des normes qui seront adoptées dans le cadre de la révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Se pose également la question de la compatibilité avec la législation suisse sur la protection des données d'un traitement en Suisse de données personnelles collectées à l'étranger de manière illicite. Les nouveaux accès en ligne prévus, à des fichiers de l'administration fédérale, ne sont pas ou pas suffisamment motivés. Enfin, nous sommes opposés à la proposition d'exclure le SRC du champ d'application de la

loi fédérale sur le principe de transparence dans l'administration (cf. ch. 2.5.4 du présent rapport d'activités).

Le projet de loi sur le renseignement est en consultation externe auprès des milieux intéressés et un message sera vraisemblablement adressé aux Chambres fédérales encore en 2013.

1.4.7 Recherche de véhicules et surveillance de la circulation automatisées

Les vérifications effectuées par les systèmes de recherche de véhicules et surveillance de la circulation automatisées de l'Administration fédérale des douanes reposent sur des bases légales adéquates. La mise à disposition par l'Office fédéral de la police d'un index contenant les numéros de plaques d'immatriculation signalées dans le système RIPOL et l'accès à cet index par les polices cantonales sont conformes au droit fédéral en vigueur. Il revient aux autorités de protection des données cantonales de se prononcer sur les vérifications effectuées dans ce contexte par les polices cantonales.

Nous avons procédé avec le Service juridique de l'Office fédéral de la police (fedpol) à l'évaluation des systèmes de recherche de véhicules et surveillance de la circulation automatisées (RSA). Nous avons examiné en particulier la conformité de ces systèmes avec la législation en vigueur. L'évaluation s'est basée sur le concept global RSA de la Commission technique des polices suisses et s'est limitée aux vérifications effectuées à partir des données du système RIPOL. Les droits d'accès en ligne à RIPOL sont réglés dans la loi fédérale sur les systèmes d'information de police de la Confédération et dans l'ordonnance sur le système de recherches informatisées de police. Ces prescriptions légales accordent explicitement des droits d'accès en ligne à des fins de recherches aux polices cantonales et à l'Administration fédérale des douanes (AFD). La mise à disposition par fedpol d'un index contenant les numéros de plaques d'immatriculation signalées dans RIPOL est également conforme au droit. Le principe de proportionnalité est lui aussi respecté. En effet, la consultation des données RIPOL n'est utilisée qu'à des fins de recherches et les installations ne couvrent pas l'ensemble du territoire (les installations fixes se limitent aux nœuds du réseau routier et les installations mobiles ne concernent qu'un nombre restreint de voitures de service). De plus, les données sont effacées immédiatement si aucune occurrence n'est trouvée. Par contre, si une occurrence est trouvée, les données sont effacées au plus tard dans

les 30 jours. Il faut également noter que l'index provenant du système RIPOL ne contient que les données absolument nécessaires et non la totalité des données. Nous avons également constaté que les polices cantonales et l'AFD respectent les prescriptions en matière de sécurité des données. On relève notamment que la transmission de l'index se fait par une connexion chiffrée et que celui-ci est conservé dans les systèmes RSA sous forme chiffrée. La mise à disposition par fedpol d'un index contenant les numéros de plaques d'immatriculation signalées dans le système RIPOL et l'accès à cet index par les polices cantonales sont ainsi conformes au droit fédéral en vigueur.

Nous avons d'autre part également examiné les vérifications effectuées par l'AFD à partir d'autres données fédérales. Ainsi, l'index des systèmes RSA de l'AFD contient les signalements de véhicules de RIPOL et les numéros d'immatriculation de véhicules impliqués dans des enquêtes relevant de la douane et des gardes-frontière. Le numéro d'immatriculation ainsi qu'une image de la plaque d'immatriculation et du véhicule ou d'une partie de celui-ci sont conservés 30 jours dans la banque de données pour la recherche de personnes. Les traitements effectués par l'AFD dans le cadre des systèmes RSA ont pour bases légales la loi sur les douanes, l'ordonnance régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'AFD et l'ordonnance sur le traitement des données personnelles dans l'AFD. Les vérifications effectuées par les systèmes RSA à partir de l'index des signalements de véhicules du système RIPOL et des numéros d'immatriculation de véhicules impliqués dans des enquêtes relevant de la douane et des gardes-frontière reposent ainsi sur des bases légales adéquates.

Il revient aux autorités de protection des données cantonales de se prononcer sur les traitements de données personnelles effectués par les polices cantonales, notamment sur les vérifications effectuées par les polices cantonales à partir de l'index des signalements de véhicules de RIPOL et à partir de données cantonales.

1.4.8 Droit d'accès aux données du système d'information ISIS: ancien et nouveau mécanisme

Du 1er janvier au 15 juillet 2012, nous avons encore traité 13 demandes d'accès selon l'ancienne réglementation. Depuis le 16 juillet 2012, les demandes d'accès au système d'information ISIS sont traitées par le Service de renseignement de la Confédération, le PFPDT étant quant à lui responsable de traiter les demandes de vérification.

Le système d'information ISIS était le dernier fichier à connaître le mécanisme dit du droit d'accès indirect. Le 16 juillet 2012, ce mécanisme a été remplacé par celui du droit d'accès direct applicable à l'ensemble des fichiers exploités par les organes fédéraux (cf. notre 19e rapport d'activités 2011/2012, ch. 1.4.4 et 1.4.5). Depuis cette date, les demandes d'accès au système d'information ISIS sont traitées directement par le maître du fichier, à savoir le Service de renseignement de la Confédération (SRC). Nous avons encore traité 13 demandes d'accès entre le 1er janvier et le 15 juillet 2012. Depuis le 16 juillet 2012, les demandes relevant du nouveau droit sont transmises au SRC pour traitement. Une fois que la personne concernée a reçu la réponse de la part du SRC, elle a la possibilité selon le nouveau droit de déposer chez nous une demande de vérification.

En ce qui concerne les demandes de vérification concernant le N-SIS et les fichiers JANUS et GEWA de l'Office fédéral de la police (fedpol), nous avons traités sept cas en 2012.

1.4.9 Essai pilote du système d'information ISAS

Le Conseil fédéral a pris connaissance du rapport d'évaluation de l'essai pilote ISAS et a autorisé la poursuite du traitement. Dans ce cadre, nous avons rendu un avis indiquant que nous n'étions pas opposés à la poursuite de l'essai pilote pour autant que le caractère limitatif du nombre de participants soit maintenu. Nous avons par contre accepté dans le cadre d'une demande spécifique du SRC sur ce point que ce nombre limité de participants soit augmenté.

En mai 2012, le Service de renseignement de la Confédération (SRC) nous a soumis pour avis un projet de rapport d'évaluation de l'essai pilote ISAS destiné au Conseil fédéral comme le prévoit l'article 17a LPD. Ce document décrit, deux ans après la mise en œuvre de la phase d'essai, le déroulement de l'essai pilote. Il mentionne également l'élaboration de la base légale au sens formel du système d'information ISAS dans le cadre d'une révision partielle de la loi fédérale sur le renseignement

civil (LFRC). Dans le projet de rapport d'évaluation, le SRC a proposé au Conseil fédéral la poursuite du traitement.

Lors de la consultation, le SRC a proposé la suppression totale de la limitation du nombre de collaborateurs concernés par l'essai pilote. Le caractère limitatif d'un essai pilote (limitation des domaines et des collaborateurs concernés) fait partie des mesures destinées à limiter les atteintes à la personnalité. La suppression du nombre maximal de collaborateurs actifs dans l'essai pilote ISAS correspondrait pratiquement à une exploitation définitive du système sans base légale adéquate. Nous nous y sommes opposés pour cette raison.

Nous avons donc examiné le projet de rapport d'évaluation et ses annexes à la lumière de ce qui précède et avons rendu un avis indiquant que le traitement des données dans le système ISAS peut être poursuivi, mais dans le cadre limité de l'essai pilote en attendant l'entrée en vigueur de la base légale au sens formel qui permettra l'exploitation définitive du système d'information ISAS. Le Conseil fédéral a pris connaissance du rapport d'évaluation et a autorisé la poursuite du traitement.

En application de l'article 27 OLPD obligeant un organe fédéral de nous informer de toute modification essentielle d'un essai pilote, le SRC nous a demandé en septembre 2012 de prendre position sur une augmentation du nombre de collaborateurs y participant. Si le caractère limitatif de l'essai pilote est essentiel et doit être maintenu comme nous l'avions rappelé dans notre avis sur le rapport d'évaluation du SRC, il convient de relever que le projet pilote ISAS se trouve dans une nouvelle phase, à savoir le développement du système d'information en vue de son exploitation définitive. Dans ce contexte et à la lumière des motifs invoqués dans la demande du SRC, une augmentation raisonnable du nombre maximal de collaborateurs du SRC participant à l'essai pilote ISAS n'a pas de conséquence significative sur les risques d'atteintes à la personnalité des personnes concernées. Pour ces raisons, nous avons émis un avis favorable concernant l'augmentation du nombre maximal de collaborateurs actifs dans l'essai pilote ISAS.

1.4.10 Loi sur la sécurité de l'information: Participation au groupe de travail FOGIS

L'ordonnance sur la protection de l'information sera remplacée à terme par une loi sur la sécurité de l'information, destinée à en élargir le champ d'application. Pour ce faire, un groupe interdépartemental a été formé. L'enjeu a consisté à harmoniser les mesures (comme la classification) de protection de l'information avec les exigences de protection des données, de transparence administrative et de sécurité physique, informatique et personnelle.

Le Conseil fédéral a décidé en date du 12.05.2010 de modifier l'ordonnance sur la protection de l'information (valable jusqu'au 31.12.2014) et de mandater le Département fédéral de la défense, de la protection de la population et des sports (DDPS) pour constituer un groupe de travail interdépartemental chargé d'établir un projet de loi sur la sécurité de l'information. Ce projet de loi doit étendre les actuelles exigences en matière de protection de l'information à la mise en œuvre des mesures pour l'amélioration de la sécurité de l'information décidées en 2009 par le Conseil fédéral. Ces mesures comportent également par nature des aspects liés à la protection des données, 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 de Markus Müller, professeur de droit à l'université de Berne.

De nombreux thèmes liés à la sécurité de l'information ont ainsi été débattus. S'agissant de la classification des informations, on peut remarquer qu'une variante à trois (interne/confidentiel/secret) et à deux niveaux (confidentiel/secret) ont été retenues. Du point de vue de la transparence administrative, c'est le modèle à deux niveaux qui convient le mieux, tandis qu'un parallèle au niveau des mesures techniques a pu être établi entre le modèle à trois niveaux et la hiérarchie «habituelle» de la protection des données personnelles (normales/sensibles/vitales). Le modèle à trois niveaux semble également mieux convenir pour les échanges d'informations classifiées avec l'étranger. Les technologies de l'information et de la communication (TIC) servant au traitement des informations classifiées ou sensibles sont quant à eux catalogués selon que le besoin de protection est général, élevé ou très élevé. Les contrôles de sécurité relatifs aux personnes traitant régulièrement des informations confidentielles ou secrètes reprennent pour l'essentiel les dispositions actuelles de la LMSI, à savoir un niveau de base, un niveau élargi et un niveau élargi avec audition. En ce qui concerne

la procédure de sécurité d'exploitation, elle exige des entreprises au contact d'informations confidentielles (ou secrètes) et de moyens TIC dignes d'un besoin de protection (très) élevé d'être au bénéfice d'une déclaration de sécurité couvrant aussi bien les risques opérationnels de sécurité, que ceux liés à son personnel par le biais d'éventuels contrôles de sécurité.

Le projet de loi issu de toutes ces réflexions, qui fera encore l'objet d'une procédure de consultation, devra également régler l'organisation interne et la coordination des nombreux offices fédéraux impliqués. Il conviendra notamment d'élaborer la stratégie fédérale pour la sécurité de l'information, d'édicter des directives techniques en matière de sécurité de l'information, d'exécuter les contrôles personnels de sécurité et les procédures de sécurité d'exploitation, de standardiser certains moyens, équipements, produits ou services de sécurité, et d'en faire annuellement rapport au Conseil fédéral. Enfin, l'exécution concernera bien entendu des organes externes comme les cantons au contact d'informations classifiées par la Confédération ou les pays étrangers avec lesquels nous échangeons des données classifiées sur la base de traités internationaux. La coordination entre organes internes et externes devra également être assurée.

Nous allons poursuivre notre participation aux travaux en cours, afin que les aspects de protection et sécurité des données, ainsi que de transparence soient pris en considération.

1.5 Santé et recherche

1.5.1 SwissDRG: certification des nouveaux services de réception de données

Pour la réception des factures de type DRG, les assureurs-maladie doivent mettre en place des services de réception des données. Ceux-ci doivent obligatoirement être certifiés au sens de la loi fédérale sur la protection des données. C'est la première fois qu'une certification en matière de protection des données devient obligatoire en Suisse.

Les forfaits par cas («Diagnosis Related Groups», abrégé DRG) constituent l'élément central du nouveau financement des hôpitaux. Les prestations des hôpitaux dans le domaine de la médecine somatique aiguë sont rémunérées en fonction de critères définis tels que le diagnostic principal, les diagnostics supplémentaires, les traitements ainsi que d'autres aspects. Pour permettre un remboursement correct des prestations par les assureurs-maladie, des factures spéciales doivent être émises. Celles-ci contiennent, en plus des données administratives, les informations médicales nécessaires sous forme codée. Cela signifie qu'avec chaque facture de type DRG, les assureurs-maladie reçoivent des données de santé détaillées sur la personne assurée.

D'un autre côté, il est évident que seule une petite partie des factures sera examinée en détail par les assureurs. C'est la raison pour laquelle un processus a dû être mis en place pour préserver la proportionnalité qui garantit que les assureurs n'aient accès aux indications médicales incluses dans la facture DRG que dans les cas où ils décident de soumettre la facture à un examen plus approfondi. Pour atteindre cet objectif, le Conseil fédéral a fixé dans l'ordonnance sur l'assurance-maladie (OAMal) que les assureurs-maladie doivent disposer d'un service de réception des données certifié au sens de la loi fédérale sur la protection des données. Ce service de réception se trouve en amont de l'assureur. Sa tâche consiste à effectuer un tri automatique des factures DRG entrantes.

Les factures y sont soumises à un contrôle de vraisemblance selon un ensemble de règles définies. En fonction du résultat, la facture sera ensuite transmise au service compétent de l'assureur. Une facture ne présentant aucune particularité est sans autre validée pour paiement, auquel cas l'assureur ne prend pas connaissance des informations médicales codées. Une facture destinée au médecin-conseil est directement transmise à ce dernier par le service de réception des données. Dans ce cas, le service de réception des données ne traite pas non plus les informations

médicales codées; il constate uniquement que la facture est destinée au médecin-conseil et se contente de la lui transmettre. L'assureur ne prend évidemment pas non plus connaissance des informations médicales. Si le service de réception des données détecte une facture présentant des particularités, il la transmet à l'assureur afin que ce dernier la soumette à un examen plus approfondi. Dans ce cas, l'assureur reçoit le jeu complet des informations médicales et peut, si cela est nécessaire pour l'examen de la facture, demander des informations complémentaires au fournisseur des prestations. Concrètement, ces informations complémentaires sont les rapports de sortie et d'opération. Ce n'est qu'ainsi qu'une facture DRG peut être proprement examinée et pas seulement soumise à un contrôle de vraisemblance. Il en va de même pour le contrôle du codage. Si l'assureur demande des informations complémentaires, il doit obligatoirement en informer la personne assurée. Celle-ci peut demander que les informations complémentaires soient transmises au médecin-conseil.

En résumé, on peut dire que le service de réception des données effectue un tri automatisé des factures DRG, ne transmet à l'assureur que les factures présentant des particularités et assure ainsi le respect du principe de proportionnalité. Le Conseil fédéral a estimé que le service de réception des données devait obligatoirement être certifié au sens de la loi sur la protection des données pour les raisons suivantes: d'une part en vue de garantir que les services de réception des données assument correctement cette tâche et n'acheminent pas un nombre trop élevé de factures à l'assureur, et d'autre part en raison du fait que le service est exploité par l'assureur ou en son nom. Etant donné que la mise en place et la certification d'un tel service nécessite un certain temps, le Conseil fédéral a prévu une solution transitoire. Tant que l'assureur ne dispose pas encore d'un service de réception des données certifié, les hôpitaux doivent transmettre leurs factures DRG uniquement au médecin-conseil. À partir du 1er janvier 2014, tous les assureurs maladie devront disposer d'un service de réception des données certifié. La transmission au médecin-conseil ne sera plus autorisée au-delà de cette date.

Cette solution constitue une étape importante du point de vue de la protection des données. D'une part, nous avons pu participer activement à l'élaboration de l'ordonnance et contribuer ainsi à la conception des mesures de protection des données des assureurs-maladie. D'autre part, la certification en matière de protection des données gagne en importance par son caractère obligatoire. Dans un secteur où l'on traite d'énormes volumes de données personnelles sensibles, les personnes chargées de ces traitements doivent impérativement être en possession d'une certification au sens de la loi sur la protection des données.

La manière dont le service de réception des données sera aménagé incombe à l'assureur et dépendra de la structure de ce dernier. Il ne fait aucun doute que de nombreux assureurs délégueront cette tâche à un prestataire externe, soit parce que l'exploitation d'un propre service de réception des données n'est pas rentable, soit parce qu'ils disposent déjà d'un prestataire externe qui effectue des traitements de données pour eux. Nous pouvons constater aujourd'hui que les grands assureurs n'auront pas besoin de la période transitoire car ils disposent déjà depuis le 1er janvier 2013 d'un service de réception des données certifié.

En ce qui nous concerne, le nouveau régime augmentera sensiblement notre charge de travail, vu que nous sommes chargés de contrôler les services de réception des données et leurs certifications. Les processus de certification varieront en fonction des cas. Etant donné que les sites peuvent être aménagés différemment en fonction des circonstances préexistantes. Nous contrôlerons également les prestataires qui se sont laissés certifier en tant que service de réception des données, tout en attachant une grande importance aux exigences spécifiques envers les certifications qui découlent du traitement des données. Ce n'est qu'avec des ressources humaines supplémentaires que le PFPDT sera en mesure de venir à bout de cette tâche complexe.

Dans un souci de transparence pour les personnes assurées, mais aussi pour la branche, nous publions depuis le 1er janvier 2013 – comme demandé par l'OAMal – la liste des services de réception des données certifiés au sens de la loi fédérale sur la protection des données.

1.5.2 Cybersanté suisse et le dossier électronique du patient: état actuel des développements

Un grand nombre d'idées issues des projets de cybersanté se concrétisent dans la loi fédérale sur le dossier électronique du patient, qui verra bientôt le jour. Nous avons participé aux travaux de conception de l'Office fédéral de la santé publique et avons réussi à influencer quelques points importants.

Au cours de cette année, le sujet cybersanté et en particulier les questions importantes relatives à la loi fédérale sur le dossier électronique du patient nous ont à nouveau fortement occupé. Il nous semble important que l'on maintienne le caractère volontaire pour les patientes et patients, que l'on garantisse leur droit à l'autodétermination informationnelle et que l'on créé un identificateur sectoriel pour la cybersanté.

À notre avis, il est crucial pour le succès du projet Cybersanté en Suisse que le patient puisse décider librement s'il désire un dossier médical électronique ou non. Une obligation dans ce domaine particulièrement sensible mettrait en péril l'ensemble du projet. Heureusement, ce concept du libre choix a été accepté par tous les groupes d'intérêts.

Si un patient opte pour un dossier électronique, son droit à l'autodétermination informationnelle doit être garanti, ce qui signifie que toute consignation au dossier nécessite son consentement. D'autre part, le patient doit avoir la possibilité, moyennant un système approprié de rôles et d'autorisations, de donner accès à ses données uniquement aux personnes de son choix. Sur le fond, cette revendication est également reconnue par les groupes d'intérêts. Ces derniers relèvent que le dossier électronique du patient pourrait toutefois perdre son utilité pratique si le personnel traitant ne peut pas compter sur le fait que les informations qu'il contient soient complètes. Nous relevons dans ce contexte qu'un médecin traitant ne peut de toute façon jamais être sûr que son patient lui révèle toutes les informations. Ce qui compte bien plus à notre avis est l'exactitude des informations effectivement contenues dans le dossier électronique du patient.

En ce qui concerne l'identificateur du patient, nous exigeons explicitement de la part de Cybersanté que le numéro d'assurance sociale (NAVS13) ne soit pas mis en relation avec les informations médicales (voir notre 19e rapport d'activités 2011/2012, ch. 1.5.2). Nous sommes à ce sujet en contact permanent avec les principaux organes. La procédure exacte n'avait pas encore été fixée à la fin de notre exercice. Une bonne solution, qui utilisera l'identificateur sectoriel que nous demandons pour l'identification des patients, semble pourtant se dessiner à l'horizon.

1.5.3 Implications de la vente de médicaments par correspondance sur la protection des données

Lors d'un examen des faits concernant des médicaments non soumis à une prescription médicale auprès d'une pharmacie de vente par correspondance, nous avons constaté que les conditions générales limitent le droit d'accès. Nous considérons cette approche comme très problématique. Son admissibilité devrait cependant être vérifiée par un tribunal.

En principe, la vente par correspondance de médicaments est interdite en Suisse. Une autorisation peut exceptionnellement être accordée si certaines conditions sont réunies pour assurer la sécurité des patients. Une de ces conditions est

qu'un médicament ne peut être remis que sur présentation d'une ordonnance. Cela signifie que les patients qui souhaitent obtenir de cette façon un médicament normalement en vente libre, doivent préalablement consulter un médecin pour qu'ils soient en mesure de présenter une ordonnance à la pharmacie de vente par correspondance. Il va de soi que certains préfèrent donc se rendre dans une pharmacie.

Une de ces pharmacies de vente par correspondance demande maintenant à ses clients qui commandent un médicament en vente libre et qui ne disposent pas déjà d'une ordonnance, qu'ils remplissent un questionnaire sur leur santé. Celui-ci sera transmis à un médecin non impliqué afin que ce dernier puisse délivrer une ordonnance qu'il transmettra à la pharmacie de vente par correspondance. Ce n'est qu'à l'issue de cette procédure que le médicament sera expédié. Les personnes qui passent commande auprès de la pharmacie doivent pour cela accepter les conditions générales de la pharmacie et déclarer qu'ils renoncent à recevoir les documents créés en interne (y compris l'ordonnance) et à connaître le nom du médecin qui a délivré l'ordonnance.

Nous avons, dans le cadre d'un examen des faits, inspecté le processus de commande et les Conditions générales de la pharmacie de vente par correspondance. La procédure doit être considérée comme très problématique, étant donné que le droit d'accès qui constitue un pilier central de la loi sur la protection des données s'en trouve fortement restreint. En fin de compte, la question qui se pose est de savoir si, dans le contexte de l'autonomie contractuelle du droit privé, le fait d'accepter les Conditions générales ne fait pas de cette limitation du droit d'accès un élément contractuel valide. Cette question devrait être tranchée par un tribunal.

1.5.4 Règlement de traitement des données des assurances: obligation de transmettre au PFPDT

Depuis le 1er janvier 2012 la loi fédérale sur l'assurance-maladie prévoit que les assureurs qui y sont soumis doivent établir des règlements de traitement des données, les soumettre à notre appréciation et les publier. Cette disposition reprend ainsi l'obligation existante dans l'article 21 de l'ordonnance relative à la loi fédérale sur la protection des données et le précise. Dans le courant de l'année 2012, nous avons procédé à un rappel concernant cette obligation auprès des assureurs qui ne nous ont pas encore transmis leur règlement de traitement.

L'article 84b de la loi fédérale sur l'assurance-maladie (LAMal) «Garantie de la protection des données par les assureurs» prévoit que: Les assureurs prennent les mesures techniques et organisationnelles nécessaires pour garantir la protection des données; ils établissent en particulier les règlements de traitement des données nécessaires conformément à l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Ces règlements sont soumis à notre appréciation et sont rendus publics.

Cette disposition reprend ainsi l'obligation existante déjà depuis 1993 en vertu de l'article 21 OLPD, mais en précisant en plus que ces règlements de traitement devront être soumis à notre appréciation et être rendus publics. En vertu de cette nouvelle disposition, les assureurs doivent donc, à partir du 1er janvier 2012, nous transmettre automatiquement leurs règlements de traitement et les publier, sur Internet par exemple ou sous une autre forme, afin d'informer les personnes intéressées. L'élaboration d'un tel règlement de traitement et sa publication par l'assureur sont obligatoires, indépendamment de notre appréciation.

L'obligation légale de ce nouvel article 84b LAMal a déjà été signalée aux assureurs par l'Office fédéral de la santé publique dans sa circulaire 7.1 du 25 août 2011. Or, constatant que de nombreuses assurances ne nous avaient pas fait parvenir leur règlement, nous avons écrit en date du 23 octobre 2012 une lettre de rappel à toutes les assurances concernées. Nous avons ainsi fixé un délai au 30 novembre 2012 aux assureurs afin de nous faire parvenir les règlements de traitement précités pour ceux qui ne s'étaient pas encore acquittés de leur obligation.

A ce jour, la plupart des assureurs concernés nous ont transmis leurs règlements de traitement.

1.5.5 Projet de loi fédérale sur l'enregistrement du cancer et autres maladies

La loi fédérale sur l'enregistrement du cancer et d'autres maladies vise à régler l'enregistrement exhaustif du cancer, sur tout le territoire suisse, en tenant compte des droits de la personnalité des patients. Les bases légales visent, par ailleurs, à créer les conditions pour la promotion de l'enregistrement des autres maladies très répandues ou dangereuses. Un tel registre doit répondre à des exigences très élevées en matière de protection des données. Nous nous sommes engagés en conséquence dans le groupe de travail et avons pris position sur le projet de loi précité.

Un groupe de travail examine la création de bases légales fédérales nécessaires à la tenue d'un registre du cancer par la Confédération. La création d'un registre du cancer représente un énorme défi du point de vue de la protection des données; nous nous sommes donc engagés en conséquence dans le groupe de travail mis sur pied sous la conduite de l'Office fédéral de la santé publique (OFSP). En effet, le Conseil fédéral a mandaté le Département fédéral de l'intérieur d'élaborer un projet de cette loi d'ici au printemps 2012. La nouvelle loi servira de base pour harmoniser les différentes législations cantonales réglementant l'enregistrement du cancer. Elle permettra en outre de recenser de manière complète et au niveau national les nouveaux cas de maladie, et de collecter des données pertinentes concernant l'évolution du cancer.

Il est ainsi prévu que les données saisies par les différents registres actuels seront transmises, sous forme cryptée, à un organe national d'enregistrement du cancer, qui sera chargé de les regrouper, de les évaluer et de les publier. Par ailleurs, la saisie des données dans les cantons devrait à l'avenir être soumise aux mêmes conditions cadres juridiques et organisationnelles. Les prescriptions proposées dans le projet de loi, permettront d'améliorer la qualité des données saisies et, partant, de simplifier les évaluations à l'échelle nationale. Les chercheurs ou des services administratifs de la Confédération et des cantons pourront accéder, sur demande, aux données anonymisées.

Nous avons eu la possibilité, dans le cadre de la consultation des offices concernant ce projet de loi, de donner notre avis. Le projet de loi prévoit la collecte pour chaque maladie oncologique d'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. Les patients seront habilités à s'opposer à la transmission des données les concernant au registre cantonal des tumeurs compétent. S'ils ne font

pas usage de ce droit, les professionnels de la santé et les institutions impliqués dans le diagnostic et le traitement des maladies oncologiques seront tenus de transmettre les données au registre cantonal compétent.

Le projet de loi prévoit, en outre, que des données supplémentaires puissent être collectées pour certaines maladies oncologiques (p. ex., évolution de la maladie, déroulement du traitement, mesures de dépistage précoce, qualité de vie). Ces données-là ne pourront être transmises au registre du cancer que si les personnes concernées y consentent. Nous avons défendu le point de vue que la collecte de ces données supplémentaires constituaient des données personnelles sensibles, soit des données qui permettent de mesurer l'évolution de la maladie, le déroulement du traitement, de même que de déterminer le milieu de vie des personnes concernées. Celles-ci, couplées avec les données minimales, permettent d'obtenir des informations très détaillées sur l'état de santé d'une personne et par conséquent constituent une atteinte particulièrement importante au droit de la personnalité et que de ce fait le médecin doit requérir le consentement explicite de son patient à la collecte de telles données.

De façon générale, nous avons réitéré nos critiques quant à l'utilisation systématique du numéro AVS en tant qu'identifiant unique. Car cela comporte 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. C'est pourquoi nous avons toujours soutenu la position qu'il était nécessaire de mettre en place un identifiant sectoriel spécifique au domaine considéré. Nous avons exprimé une nouvelle fois notre réserve à l'introduction du numéro AVS dans les registres cantonaux des tumeurs. 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 de numéros spécifiques à chaque domaine réduit le risque que les informations soient mises en relation, d'autant plus que les données des registres des tumeurs sont sensibles et permettent l'établissement de profils de la personnalité. A toutes fins utiles, nous avons également rappelé que le 18 avril 2012, le Conseil fédéral a chargé l'OFSP d'étudier, notamment en collaboration avec la Centrale de compensation des alternatives à l'utilisation du numéro AVS pour l'identification des patients dans le cadre de l'avant-projet de la loi fédérale sur le dossier électronique du patient. Il nous apparaît dès lors nécessaire que les travaux menés dans ce contexte soient aussi pris en compte dans le cadre de ce projet d'enregistrement du cancer.

Nous avons également mis en évidence que l'appariement de données des registres des tumeurs cantonaux avec les données de la statistique de l'Office fédérale de

la statistique (OFS) devait respecter les exigences de l'article 14a alinéa 2 de la loi sur la statistique fédérale (LSF). Il s'agit ici d'éviter tout appariement des données non autorisé. Pour rappel, le législateur a limité le droit d'appariement de données à l'OFS et aux offices statistiques cantonaux et communaux dans le but de garantir la protection des données et d'éviter que des profils de personnalité ne puissent être établis. Par ailleurs, l'appariement de données est prévu dans un but statistique et non administratif comme c'est ici le cas. De plus, l'appariement de données par l'OFS doit respecter les conditions de l'article 14a LSF, à savoir que les données doivent être anonymisées. Par ailleurs, l'utilisation du numéro AVS par l'OFS nécessite encore des travaux législatifs (qui prendront la forme d'une révision partielle de la LSF) afin de permettre une règlementation uniforme du numéro AVS dans les relevés statistiques.

L'OFSP a pris en compte l'essentiel de nos remarques. Notre divergence exprimée durant la consultation des offices quant à l'utilisation du numéro AVS a été reprise dans la proposition au Conseil fédéral. Lors de sa séance du 7 décembre 2012, le Conseil fédéral a approuvé le projet de loi et a ouvert la procédure de consultation externe. Nous continuerons à suivre attentivement ces travaux législatifs.

1.5.6 Activité de surveillance dans le domaine de la recherche médicale

Dans le domaine de la recherche médicale effectuée à l'aide de données personnelles de patients, les personnes concernées ne sont pas toujours invitées à donner leur consentement. Nombre de personnes concernées ne savent pas qu'elles ont un droit de veto.

En principe, les données de patients ne peuvent être utilisées pour la recherche que si ceux-ci ont donné leur consentement après information et délai de réflexion. Il existe cependant des cas dans lesquels les patients restent introuvables, p. ex. lorsqu'ils ont déménagé à l'étranger ou qu'ils sont décédés. Il n'est plus possible alors d'obtenir leur consentement. Au-delà d'un certain nombre de personnes impliquées dans un projet de recherche, leur consentement n'est plus exigé. En outre, il peut être intolérable pour un (ancien) patient qu'on lui demande un tel consentement, par exemple dans les cas où cela concerne une grave maladie qu'il a subi et qui l'a fortement touché sur le plan émotionnel. Dans ces cas, où aucun accord ne peut (ou ne doit) être obtenu, une autorisation peut être demandée auprès de la Commission d'experts du secret professionnel en matière de recherche médicale.

Les personnes concernées ont en outre un droit de veto et de rétraction. Elles doivent être rendues attentives au fait que leurs données peuvent être utilisées à des fins de recherche, qu'elles ont le droit de faire bloquer ces données (droit de veto) et qu'elles peuvent révoquer leur consentement à une date ultérieure. Avec des annonces dans les journaux quotidiens ainsi que dans les informations accompagnant les médicaments, les hôpitaux attirent l'attention de la population ou des patients sur cette utilisation des données du patient à des fins de recherche. Des sondages effectués auprès de personnes potentiellement concernées ont pourtant révélés qu'aucune des personnes interrogées n'était consciente du fait que ses données pouvaient également être utilisées à des fins de recherche. Il semble que les patients ou la population en général ne prennent pas suffisamment connaissance de ces informations. Cette situation pose problème puisque les personnes concernées doivent être informées de manière à ce qu'elles puissent se former une image claire du traitement de données, surtout lorsque celui-ci concerne des données sensibles, et que cette information est la condition requise pour qu'ils puissent donner leur consentement. L'information du patient doit commencer au moment de la collecte des données et ne se termine qu'une fois que les données ont été détruites ou anonymisées. Si la personne concernée se fait une fausse idée du traitement de données sur la base des informations qu'elle a reçues, il y a un risque que le consentement ne soit pas considéré comme étant légal.

En ce qui concerne le droit de veto, il y a lieu de relever que les patients sont confrontés à un dilemme. S'ils savent qu'ils disposent d'un droit de veto et qu'ils en font usage, ce dernier vaut généralement pour tous les projets de recherche. Souvent, le patient est cependant conscient qu'un grande partie des projets de recherche est importante et ne veut donc pas forcément s'opposer à tous les projets de recherche. Cela signifie donc qu'il préférera ne pas faire usage de son droit de veto. Ce faisant il est pourtant prêt à accepter, conformément aux conditions susmentionnées, le risque que ses données soient utilisées à son insu à des fins de recherche. Une approche probablement plus appropriée et mieux applicable consisterait à pseudonymiser les données des patients pour les mettre à disposition des chercheurs sous une forme qui ne permette plus d'identifier la personne. Une telle approche ne nécessiterait plus le consentement des personnes concernées. Un consentement ne devrait être obtenu que dans les cas où il s'avérerait nécessaire de collecter d'autres données auprès du patient. Une telle démarche serait plus simple et aussi plus transparente. Des solutions possibles ont déjà été élaborées. Comme nous l'avons indiqué dans notre 16e rapport d'activités 2008/2009 au ch.1.5.4, vous les trouverez sur le site web de

la TMF (Technologie- und Methodenplattform für die vernetzte medizinische Forschung) http://www.tmf-ev.de/ (en allemand). Vous y trouverez également, dans la rubrique «Schriftenreihe» [Publications], l'ouvrage «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin».

1.6 Assurances

1.6.1 Procédure d'établissement des faits auprès d'un assureur-maladie

Les assurances-maladie doivent permettre à leurs collaborateurs d'accéder aux données médicales des assurés afin d'établir les décomptes de prestations. Dans l'idéal, le collaborateur a accès aux données dont il a besoin pour le cas à traiter. Le droit d'accès devrait être retiré lorsque le décompte est clos. Mais l'idéal fait rarement partie de la réalité. C'est ce que montre une procédure d'établissement des faits, menée auprès d'un grand assureur-maladie.

Un cas d'infraction présumée à la loi sur la protection des données, dont l'auteur serait un grand assureur-maladie, nous a été communiqué: presque tous les collaborateurs avaient accès à des données sensibles d'assurés. Si le grief était véridique, il se serait agi d'une grave violation des droits de la personnalité des assurés. Nous avons donc décidé d'examiner en détail l'état des faits.

Une prise de position écrite de l'assureur n'a pas permis de répondre à toutes les questions. Par contre, un examen de la situation sur place a clarifié la situation. Il est apparu que le reproche formulé était juste. Plusieurs centaines de personnes avaient accès aux données des assurés, dont des collaborateurs qui n'avaient rien à voir avec le cas traité en l'espèce. Nous sommes parvenus à convaincre l'assureur que son programme d'accès devait être modifié d'urgence pour répondre aux exigences du droit de la protection des données. Or, cette adaptation de logiciel pour les décomptes de prestations s'avèrent très coûteux. Ainsi, il se pourrait qu'à l'avenir, plusieurs grands assureurs appliqueront les mêmes règles, et surtout des règles acceptables. C'est là, à nos yeux, un procédé fort louable. Au cours du premier semestre 2013, l'assureur nous remettra le projet de base en vue d'une solution pour le futur. Nous l'examinerons d'un œil critique et en contrôlerons la mise en œuvre.

1.6.2 Sondage sur le don d'organes par une assurance

Notre attention a été attirée sur une pratique mise en place par une assurance s'agissant de donner son avis sur le don d'organes. Dans ce cadre-là, nous avons ouvert une procédure d'éclaircissement des faits. Nous avons pu constater que l'assurance concernée avait entrepris les démarches en vue de satisfaire aux exigences de la législation sur la protection des données. Nous avons toutefois signalé à l'assurance des points à prendre en compte dans le cadre d'éventuels futurs sondages.

Dans le cadre de nos activités de conseil et d'information, nous sommes régulièrement confrontés à de nombreuses sollicitations émanant du public qui sont intéressés par notre position sur certains traitements de données effectués par des sociétés, des personnes privées ou des organes fédéraux. Nos prises de position dans ces situations-là ont en principe un caractère général avec pour but de sensibiliser le public sur les dangers potentiels d'un traitement de données, sans préjuger d'un cas d'espèce concret.

Dans ce contexte, nous avons été abordés plusieurs fois afin de connaître notre avis sur les conditions de participation au sondage organisé par cet assureur, notamment en relation avec la collecte de certaines données personnelles (tel que le numéro AVS du participant) et leurs transmissions sur le site d'une société américaine hébergeant le sondage.

Indépendamment du cas d'espèce, nous avons fait part de nos appréhensions globales liées à la problématique générale de la transmission de données à destination de pays dont la législation n'assure pas un niveau de protection adéquat, tels les Etats-Unis, et avec lesquels aucune garantie suffisante n'aurait été prise. Dans le cadre de notre activité, nous constatons fréquemment que cette problématique est souvent ignorée de nombreuses personnes physiques ou entreprises envisageant le transfert des données personnelles sensibles (comme les données liées à la santé d'une personne) dans ces pays. Par cette démarche, la protection de la sphère privée des personnes concernées n'est bien souvent plus assurée et les risques d'atteinte à la personnalité sont accrus.

Vu l'ampleur du sondage et au regard de notre expérience relative aux risques potentiels liés au traitement de données effectués aux Etats-Unis, nous avons procédé à un éclaircissement des faits, conformément à l'article 29 de la loi fédérale sur la protection des données (LPD) afin d'avoir une idée plus concrète des mesures prises par l'assurance pour garantir la protection des données des participants.

Suite à l'analyse des explications et de la documentation remise par l'assureur, ainsi qu'au contrôle effectué sur le site du sondage, nous avons pu constater que l'assurance a entrepris les démarches en vue de satisfaire aux exigences de la LPD. En ce qui concerne le motif justificatif (consentement des participants au traitement de leurs données personnelles dans le cadre du sondage). En outre, des garanties contractuelles ont été prises dans le cadre de communications transfrontalières permettant d'assurer un niveau de protection adéquat à l'étranger (adhésion de la société américaine hébergeant le site du sondage au US-Swiss Safe Harbor Framework).

Nous avons toutefois attiré l'attention de l'assurance sur le fait que l'utilisation systématique du numéro AVS en dehors des assurances sociales n'est licite qu'aux conditions définies par l'article 50e de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS), soit dans des domaines qui sont étroitement liés aux assurances sociales. L'utilisation du numéro AVS en dehors de ce contexte est possible si une base légale ad hoc est créée, respectivement au niveau de la Confédération ou à celui des cantons. L'habilitation à utiliser le numéro AVS est donnée directement par le législateur qui a entendu règlementer clairement le champ d'application du numéro d'assuré en précisant: «Ce qui est sûr, c'est que de nombreux utilisateurs se servent systématiquement du numéro AVS. Il n'y a cependant pas de vue d'ensemble des domaines d'utilisation et il n'est pas possible d'en constituer une qui serait fiable. Cet état de fait contrevient à l'exigence de contrôle et de possibilité de contrôle posée par le droit de la protection des données. Partant, il semble indispensable de réglementer clairement le champ d'application du numéro d'assuré. Dorénavant, les utilisations à des fins purement privées ne devraient plus être possibles». En fixant des conditions d'utilisation strictes, cette législation a été adoptée dans l'esprit de prévenir les risques liés à un usage incontrôlé du numéro AVS en tant qu'identifiant unique pour la sphère privée des personnes concernées, en raison des connexions indésirables que cette extension permet d'établir entre différentes bases de données.

Par ailleurs, si nous avons pris note du fait que la société américaine hébergeant le site internet du sondage a adhéré au contrat US-Swiss Safe Harbor Framework et qu'elle s'est enregistrée sur le site du département du commerce américain, nous avons toutefois rappelé que l'article 6 LPD concernant la communication transfrontière de données ne règle que la question du caractère transfrontalier de la communication. Celle-ci doit dans tous les cas respecter les principes généraux de la LPD (art. 4, 5 et 7). Il ressort de notre examen que dans le cadre de ce sondage, si les participants reçoivent bien de manière adéquate une information sur les buts de ce sondage et sur les traitements de données y relatifs, ils devraient être

clairement informés par l'assurance que leurs données personnelles font l'objet d'une communication aux Etats-Unis. Seul un utilisateur particulièrement avisé et attentif peut se rendre compte que le sondage est effectué au moyen du site de la société américaine sans pour autant savoir que ses données personnelles sont hébergées sur le serveur de cette société aux Etats-Unis.

A la lumière de ce qui précède, nous avons donc conclu que le sondage remplissait les conditions mises par la LPD en ce qui concerne son motif justificatif et les garanties permettant d'assurer un niveau de protection adéquat à l'étranger, mais avons toutefois relevé qu'un tel sondage effectué par une entreprise ne pouvait pas faire usage du numéro AVS et que les participants devaient être clairement informés de la communication de leurs données personnelles à l'étranger. Vu que le sondage en cause est terminé, nous avons considéré qu'il n'y a pas lieu d'émettre de recommandation au sens de l'article 29 alinéa 3 LPD mais qu'il appartient cependant à l'assurance de prendre en compte les considérations développées ci-avant dans le cas d'éventuels futurs sondages.

1.7 Secteur du travail

1.7.1 Exigences envers un système pour lanceurs d'alertes

La Suisse ne connaît pas d'exigences légales pour la mise en service au sein d'une entreprise privée d'un système pour lanceurs d'alerte. Dans le cadre de notre service d'assistance téléphonique, nous avons dû répondre à plusieurs questions concernant ce sujet. Une des questions souvent posées était aussi de savoir s'il existe une obligation de déclarer les fichiers d'un système pour lanceurs d'alerte. Nous avons retenu qu'il était indiqué d'annoncer de tels fichiers.

Nous avons reçu à plusieurs reprises des demandes téléphoniques émanant d'entreprises ou de leurs représentants légaux pour savoir s'il existait en Suisse des bases légales spécifiques pour la mise en place et l'exploitation d'un système pour lanceurs d'alerte. Au sein de l'administration fédérale, nous avons depuis janvier 2011 l'article 22a de la loi sur le personnel de la Confédération. Pour le secteur privé, il n'existe pas de règlementations spécifiques, mais il y a lieu de respecter notamment les dispositions de la loi sur la protection des données.

Pratiquement chacune de ces demandes incluait la question de savoir si les fichiers relatifs à un tel système devaient être annoncés. Un particulier doit nous annoncer un fichier dans les cas où celui-ci traite régulièrement des données personnelles sensibles ou des profils de la personnalité ou si des données personnelles sont communiquées à des tiers. Il n'est pas à exclure, voire même très probable que, sur la base des annonces reçues, l'exploitation d'un système pour lanceurs d'alerte traite régulièrement des données personnelles sensibles. Même si cela ne correspond pas à la volonté de l'exploitant, il n'a pas vraiment la possibilité de l'influencer. Au vu de ces faits, nous avons toujours recommandé aux personnes qui nous ont appelées d'annoncer leur fichier.

1.7.2 Envoi de certificats de caisse de pension – arrêt du Tribunal administratif fédéral et suivi du contrôle

Le 12 avril 2012, le Tribunal administratif fédéral a jugé que les certificats de caisse de pension devaient à l'avenir être remis de manière que seule la personne assurée, à l'exclusion de tout tiers, puisse en prendre connaissance. La mise en œuvre de ce jugement a fait l'objet d'une vérification de notre part.

Le PFPDT a d'ores et déjà critiqué à maintes reprises la pratique appliquée par les institutions de prévoyance dans le cadre de la remise des certificats de caisses de pension à leurs assurés (cf. notre 17e rapport annuel 2009/2010, ch. 1.7.8 et notre 18e rapport annuel 2010/2011, ch. 1.7.3). Un bref rappel des évènements: en 2009, nous avons ouvert une procédure d'établissement des faits dans l'affaire cité sous titre et recommandé à l'institution de prévoyance concernée d'effectuer un envoi direct et exclusif des certificats aux personnes assurées. Cette recommandation n'a toutefois pas été suivie par la caisse de pension. Etant donné que cette dernière agit en qualité d'organe fédéral, nous avons, conformément à la procédure applicable dans le cadre de la surveillance des organes fédéraux, déposé une demande de décision en la cause auprès du Département fédéral de l'Intérieur (DFI). Le DFI a pour sa part approuvé la pratique de la caisse de pension ce qui nous a contraint à formuler un recours contre sa décision auprès du Tribunal administratif fédéral. Le recours a été admis le 12 avril 2012 (cf. notre 19e rapport d'activités 2011/2012, ch. 1.7.2). L'arrêt A-4467/2011 du TAF, qui est désormais entré en force de chose jugée, a pour conséquence que les certificats doivent à l'avenir être remis de manière que seule la personne assurée – à l'exclusion de tout tiers, notamment l'employeur – puisse prendre connaissance du contenu de ce certificat.

Nous avons examiné l'application de l'arrêt dans les locaux de l'institution de prévoyance le 19 décembre 2012 dans le cadre d'un contrôle. Le constat a été le suivant: les critères d'envoi répondent désormais aux conditions exigées par le TAF. Toutes les parties potentiellement impliquées dans le processus d'envoi (fonds de prévoyance professionnelle des entreprises, employeurs, employés, courtiers, etc.) ont été informés par l'institution concernée que les certificats seraient dorénavant expédiés directement à l'employé dans des enveloppes scellées portant la mention «personnel».

Cet arrêt du Tribunal administratif fédéral arrive à point nommé, car il renforce la sécurité du droit en ce qui concerne la transmission de données dans un domaine important comme la prévoyance.

1.7.3 Communication aux autorités américaines de données concernant des collaborateurs

Diverses banques ont transmis aux autorités des Etats-Unis des documents qui contenaient des noms, adresses de courriel et numéros de téléphone de collaborateurs actuels ou anciens ainsi que de tierces personnes. Nous avons pour cette raison procédé à un examen des faits auprès des cinq banques concernées, à la suite duquel nous avons émis des recommandations demandant aux banques d'adopter une démarche plus transparente.

Dans le cadre de négociations en cours avec les Etats-Unis, plusieurs banques suisses avaient transmis aux autorités de ce pays des documents concernant des affaires traitées avec des clients américains. Ces documents contenaient entre autres les noms d'actuels ou d'anciens collaborateurs ainsi que de tierces personnes. Plusieurs de ces personnes se sont adressées à nous. Après avoir appris que d'autres communications de données avaient été effectuées par des banques, nous avons décidé en août 2012 d'effectuer un examen des faits afin de tirer au clair les questions touchant à la protection des données. Le but de cette procédure était d'obtenir une vue d'ensemble des communications de données effectuées afin de pouvoir évaluer si celles-ci avaient violé des droits de la personnalité ou de déterminer comment on pouvait mieux protéger les personnes concernées.

Cet examen des faits nous a mené à avoir des entretiens avec le Secrétariat d'Etat aux questions financières internationales, la FINMA et l'Office fédéral de la justice. On nous y a exposé les considérants qui ont amené le Conseil fédéral à prendre ses décisions concernant la coopération des banques avec les autorités des Etats-Unis. Nous avons également reçu les banques impliquées. Comme première mesure, nous leurs avons demandé d'adopter une attitude transparente envers leurs collaborateurs afin de protéger les personnes concernées. Les banques se sont engagées en conséquence, pendant la durée des enquêtes en cours, à informer les collaborateurs avant chaque livraison de documents aux autorités américaines au cas où leur nom devait y figurer. Les banques ont en outre dû remplir un questionnaire et nous fournir une description de la procédure appliquée pour la livraison des documents et l'information des collaborateurs. Dans quelques-unes des banques, nous nous sommes rendus sur place afin de nous faire présenter la démarche appliquée pour la sélection des documents et la procédure relative à l'information et au droit d'accès des collaborateurs.

Sur la base des documents qui nous ont été remis et des explications données, et au vu des organes fédéraux impliqués, nous avons conclu que les communications de données étaient compréhensibles dans le contexte d'un intérêt public prépondérant. On nous a expliqué de manière crédible que les banques risquaient de subir de graves conséquences au cas où elles refuseraient de transmettre les informations demandées par les autorités américaines. Dans nos recommandations, nous avons donc approuvé l'intérêt public prépondérant, qui est une condition préalable à la communication de données personnelles vers un pays ayant un niveau de protection des données insuffisant. Dans le même temps, nous avons cependant clairement démontré que les banques n'ont pas agi en conformité avec les exigences de la protection des données lors des livraisons de données déjà effectuées. Ainsi, les instituts n'ont pas tous informé toutes les personnes concernées des livraisons de données imminentes. D'autre part, l'accès aux documents transmis n'a pas été donné à toutes les personnes concernées. C'est pour cette raison que nous avons inclus dans nos recommandations l'exigence envers les banques de donner aux personnes concernées (collaborateurs actuels ou anciens ainsi que tiers externes) l'accès aux documents qui ont déjà été livrés. Pour toute livraison future de données aux autorités américaines, les banques devront informer les personnes concernées à l'avance sur l'envergure et la nature des documents devant être transmis ainsi que sur la période dont ces derniers datent. Les banques doivent également informer les anciens employés et les parties externes, dans la mesure où ceci est possible moyennant un effort raisonnable.

Elles doivent ensuite accorder aux personnes concernées un délai raisonnable, dans lequel elles peuvent demander des renseignements sur tous les documents qui les concernent. Si la personne se prononce envers la banque, suite aux renseignements obtenus, contre une transmission des documents qui contiennent son nom, la banque devra peser les intérêts en jeu pour le cas d'espèce. Si une banque désire néanmoins transmettre les documents avec le nom de la personne concernée, elle devra l'informer de cette livraison ainsi que de ses droits.

Toutes les banques impliquées ont accepté nos recommandations. Celles-ci peuvent être consultées sur notre site www.leprepose.ch sous Protection des données – Recommandations (en allemand).

1.7.4 Systèmes de surveillance et de contrôle sur le lieu de travail

L'évolution de ces dernières années dans le domaine de l'électronique a entraîné d'importants changements dans le monde du travail. Les employeurs disposent aujourd'hui d'un arsenal de plus en plus important d'instruments de surveillance et de contrôle. Ceci soulève la question de savoir quels types de surveillance sont acceptés et quels contrôles vont trop loin.

Conjointement avec une équipe de projet du Secrétariat d'Etat à l'économie (SECO), qui s'est occupée de la surveillance technique des personnes à leur lieu de travail, nous avons collaboré à la révision de la directive sur l'ordonnance 3 relative à la loi sur le travail, concernant l'article 26. Selon cet article, il est en principe interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur lieu de travail.

Les données personnelles peuvent être collectées uniquement de manière légale. Leur traitement est régi par le principe de bonne foi et doit être effectué selon les dispositions de la loi sur la protection des données et de l'ordonnance y afférente. Le principe de la proportionnalité doit toujours être respecté. Il ne peut être traité que des données qui sont en relation avec le but du traitement. Celles-ci doivent en outre être détruites dans un délai le plus bref possible, défini à l'avance. L'accès aux données personnelles traitées (fichier) doit faire l'objet d'une réglementation. Il doit être limité aux personnes qui sont autorisées à avoir accès à ces données.

Lors de l'utilisation de systèmes de surveillance ou de contrôle, il faut toujours veiller à garantir la protection de la personnalité des collaboratrices et des collaborateurs. Les personnes concernées doivent être informées au préalable sur la nature, le but et la finalité du traitement de données. Si possible, on élaborera un règlement d'utilisation interne à l'entreprise qui informe de manière transparente les collaboratrices et collaborateurs sur leurs droits et obligations lors de l'utilisation de systèmes de surveillance ou de contrôle. Il s'est avéré que de tels systèmes ne sont pas uniquement utilisés pour des raisons internes à l'entreprise, mais qu'ils peuvent également contribuer efficacement à améliorer la protection et la sécurité du personnel en général. L'employeur consciencieux doit cependant toujours se rappeler qu'une utilisation de tels systèmes sans annonce préalable éveille la méfiance. Néanmoins, un contrôle raisonnable et concevable peut sans autre être justifié. Un contrôle est notamment considéré comme étant raisonnable et concevable lorsque la transparence est de mise et que l'on ne découvre pas avec

surprise un «espionnage». Si le principe de la transparence n'est pas respecté, les collaboratrices et collaborateurs chercheront un soutien.

L'utilisation de systèmes de surveillance ou de contrôle au lieu de travail touche deux catégories de problèmes. Dans la mesure où la surveillance et le contrôle portent principalement sur le comportement des collaborateurs, où leur santé est donc compromise, et où la protection de la personnalité demeure l'objectif principal, on s'adressera tout d'abord aux offices cantonaux de l'inspection du travail. Dans les cas par contre où l'accent porte sur la collecte et le traitement de données personnelles, on n'hésitera pas à consulter en plus le responsable de la protection des données.

1.7.5 Gestion du compte de messagerie dans la vie professionnelle

Qui gère le compte de messagerie lors d'une absence imprévue? Dans quelle mesure mon employeur est-il autorisé à consulter mes courriels? Voici quelques exemples de questions que les employés nous posent fréquemment sur notre ligne d'assistance téléphonique. La protection de l'intégrité personnelle et de la sphère privée dans le monde du travail doit faire l'objet d'une réglementation.

L'emprise croissante de l'informatique a fortement modifié le travail quotidien au bureau. Alors qu'il était autrefois relativement facile de respecter la sphère privée, ceci n'est plus le cas aujourd'hui. Du temps où la correspondance n'arrivait que par courrier postal ou par coursier, on appliquait la règle contraignante selon laquelle les enveloppes marquées «personnel» ne devaient pas être ouvertes par le personnel administratif responsable du tri du courrier. Les employés avaient à leur disposition une boîte aux lettres personnelle qu'ils pouvaient verrouiller et dans lequel ils pouvaient conserver leur courrier personnel. L'accès à la correspondance relative à l'entreprise devait cependant toujours être assuré, même si une collaboratrice ou un collaborateur était absent, soit à la place de travail, soit dans un classement centralisé.

Ce système continue à fonctionner sans problème pour le courrier postal et les documents reçus par coursier. Mais depuis que les collaborateurs disposent de leur propre compte de messagerie électronique, la majorité des informations, autant professionnelles que privées, sont échangées par ce moyen. Le courrier électronique remplace de plus en plus le courrier postal. Malheureusement, nombre d'entreprises ne différencient pas clairement entre les courriels privés et ceux qui concernent l'entreprise. Très souvent, ce n'est que lors d'un cas d'absence imprévue

d'une personne, que ce soit pour cause de maladie ou d'accident, que l'on se pose la question fondamentale de savoir si l'employeur est en droit d'ouvrir le courrier électronique de cette dernière sans avoir auparavant demandé son assentiment. Il s'agit là d'une des questions que l'on nous pose le plus fréquemment sur notre ligne d'assistance téléphonique. Il serait donc préférable que l'employeur définisse dans un règlement relatif à l'utilisation du système informatique de l'entreprise la manière dont les collaboratrices et collaborateurs peuvent utiliser leur compte de messagerie. Le droit de donner des instructions, selon l'article 321d du Code des obligations, lui en fournit la base légale nécessaire.

Un tel règlement d'utilisation assure la transparence et la sécurité du droit. Le personnel doit savoir quelles sont les compétences dont dispose l'employeur, afin d'éviter des discussions inutiles entre celui-ci et ses employés. Si des règles sont édictées, on veillera également à ce qu'elles soient appliquées. Une interdiction totale de l'usage du courrier électronique à des fins privées nécessiterait un énorme effort de contrôle, raison pour laquelle une telle interdiction reste la plupart du temps illusoire. Plus un règlement d'utilisation est clair, plus le personnel sait ce qui est permis et ce qui ne l'est pas. La solution idéale consisterait à séparer rigoureusement les courriels professionnels des courriels privés. Etant donné que l'entreprise ne met généralement pas deux adresses de courriel à disposition de leurs collaborateurs, une pour le courriel d'entreprise et une pour le courriel privé, on peut exiger des collaborateurs qu'ils déplacent immédiatement leurs messages privés vers un dossier personnel séparé, p. ex. en définissant une règle appropriée dans leur compte. Lors d'absences prévues, les collaborateurs activeront le gestionnaire d'absence du bureau de leur compte de messagerie. Lors d'absences imprévues de longue durée, les responsables informatiques devraient avoir la possibilité d'activer le gestionnaire d'absence du bureau ou de dévier les courriels entrants sans devoir pour cela ouvrir le compte de messagerie de la personne absente.

Vous trouverez d'autres solutions possibles dans notre «Guide relatif à la surveillance de l'utilisation d'internet et du courrier électronique au lieu de travail» sur notre site www.leprepose.ch sous Protection des données – Documentation – Guides.

1.7.6 Assurance qualité conforme à la protection des données dans un institut privé d'études de marché

Suite à notre intervention, un institut privé d'études de marché auprès duquel nous avions effectué un examen des faits l'année dernière, a mis en œuvre une procédure qui prévoit une assurance qualité conforme aux exigences de la protection des données.

Dans le cadre d'un examen des faits effectué auprès d'un institut d'études de marché (cf. notre 19e rapport annuel 2011/2012, ch. 1.1.1), nous avons constaté que les employés étaient dans certains cas mal informés sur la façon dont la qualité de leur travail était contrôlée. Ainsi, leurs supérieurs ont écouté des interviews sans en informer la personne qui menait l'interview. De plus, la procédure d'écoute n'était pas réglée de manière uniforme et transparente pour les collaborateurs. Un tel «Silent Monitoring» peut toutefois constituer une surveillance systématique disproportionnée, ce qui est inacceptable du point de vue du droit du travail.

Dans le cadre de l'examen des faits auquel nous avons procédé l'année dernière, nous avons rendu l'entreprise attentive à ce problème, sur quoi cette dernière a élaboré une nouvelle procédure uniforme et clairement définie pour l'assurance qualité. Celle-ci prévoit que les collaborateurs seront désormais avertis par un signal optique lorsque leur conversation est écoutée par un supérieur. Un «Silent Monitoring» sans préavis n'est possible que dans certaines situations exceptionnelles, notamment pendant la période d'essai ou dans des cas où les prestations fournies sont insuffisantes. Les exceptions possibles sont communiquées de manière transparente au personnel. Nous jugeons cette manière de procéder comme étant conforme aux exigences de la protection des données. Après avoir vérifié la documentation de cette procédure et reçu la confirmation qu'elle était bien appliquée dans l'entreprise, nous avons pu clore l'enquête. Sur la base de cette expérience, nous nous attendons à ce que d'autres entreprises actives dans ce domaine adaptent à l'avenir leur assurance qualité afin de la rendre conforme aux exigences de la protection des données.

1.7.7 Code de comportement visant à prévenir les conflits d'intérêts des employés fédéraux

Le nouveau code de comportement de l'administration fédérale prévoit que les employés doivent déclarer leur participation dans des entreprises privées dès que celle-ci dépasse un certain montant. On nous a demandé si une telle déclaration était compatible avec les principes de la loi sur la protection des données.

Suite à la démission du président de la Banque nationale au début de 2012, plusieurs organes fédéraux ont jugé opportun d'élaborer un code de conduite ou un règlement en vue d'éviter les délits d'initiés et les conflits d'intérêts. Un de ces organes nous a remis son projet de code en nous demandant de l'évaluer du point de vue de la protection des données. Ce code de conduite prévoyait une obligation de déclarer les participations privées à partir d'un certain montant. Dans une première prise de position, nous avons surtout examiné la manière dont la déclaration ou le contrôle devait être effectué.

Nous avons retenu que les données ne pouvaient pas, dans le cadre d'une telle obligation de déclaration, être communiquées sans autre à un tiers, telle qu'une agence fiduciaire, sans qu'une base légale le permette. L'organe en question a par la suite renoncé à une telle communication.

Dans une deuxième étape, nous avons demandé à l'unité administrative de prendre position en ce qui concerne les bases légales existantes relatives au devoir d'information. Sa réponse indiquait que l'obligation de déclaration était basée principalement sur l'article relatif au devoir de fidélité de la loi sur le personnel de la Confédération (art. 20 LPers). Au moment où nous avons reçu cette demande, cet article n'était mentionné dans l'ordonnance qui s'y rapporte (OPers) que pour les activités accessoires. L'unité administrative a cependant relevé que, lors de la révision de l'OPers en automne 2012, cet article serait amendé par des dispositions relatives à l'acceptation d'activités accessoires et à d'autres obligations du personnel. Elle a également rendu attentif au fait que les départements et unités administratives pourront alors édicter des dispositions complémentaires, notamment pour prévenir les conflits d'intérêts et l'utilisation abusive d'informations confidentielles.

Sur la base de ces explications et au vu de la révision de l'OPers dans ce domaine, nous avons conclu qu'une communication de participations privées dépassant un certain montant pouvait sans autre être exigée dans le service concerné. De telles obligations des employés peuvent maintenant, en vertu de la base légale

existante (article 14 OPers, en vigueur depuis le 15 septembre 2012), être stipulées de manière conforme aux exigences de la protection des données dans des dispositions complémentaires telles que directives, code de comportement ou règlement, et les données peuvent également être traitées ensuite par le service en question.

1.8 Economie et commerce

1.8.1 Analyse du panier pour les programmes de fidélisation des clients

Sur demande d'un grand distributeur, nous avons examiné du point de vue de la protection des données l'introduction postérieure, sur la carte-client, d'une analyse du panier des achats. Une telle modification du traitement des données doit répondre à des critères particulièrement stricts quant à la transparence et au consentement des clients.

De nombreuses entreprises utilisent les cartes-clients dans le cadre de leurs programmes de fidélisation. Les participants bénéficient de certaines réductions et autres avantages; en contrepartie, l'entreprise entend attacher le plus possible ses clients à ses prestations. L'entreprise enregistre donc sur la base de l'analyse du «panier de la ménagère» les achats que les clients ont payés en présentant leur carte-client. L'entreprise rassemble ainsi des données détaillées sur les produits achetés et peut planifier des mesures de marketing ou autres. Il faut que les participants à ces programmes de fidélisation soient informés de manière transparente de la récolte de leurs données. Ils peuvent toutefois directement influencer la collecte de leurs données d'achat eux-mêmes en présentant ou pas leur carte-client.

Au début de l'année, un grand distributeur nous a demandé d'examiner du point de vue de la protection des données l'introduction postérieure d'une analyse du panier des achats de leurs clients. Jusque-là, l'entreprise n'avait sauvegardé les données d'achats que dans un but de comptabilité. Nous avons souligné à son intention que l'introduction d'une telle mesure à des fins de marketing permettait d'établir des profils de la personnalité au sens de la loi sur la protection des données (LPD). Plusieurs conditions doivent être respectées dans ce contexte: l'entreprise doit informer ses clients de manière complète et transparente de la modification envisagée. Outre l'information rajoutée dans les conditions générales relatives à la carte-client, l'entreprise doit utiliser d'autres vecteurs d'information comme le site internet ou le magazine-client. Pour leur part, les utilisateurs de la carte doivent approuver expressément l'analyse de leur panier après avoir pris connaissance de ces modifications. Il ne suffit pas à ce propos que le client continue simplement d'utiliser sa carte. Le consentement à l'analyse du panier des achats doit ressortir directement de la déclaration (par exemple le client coche une confirmation pré-formulée). En l'absence de ce consentement, il faut s'abstenir

de toute analyse du panier de la personne concernée. Les clients ne doivent pas être contraints d'approuver les nouvelles dispositions. De même, les participants au programme de fidélisation doivent avoir la possibilité de ne pas recevoir des propositions publicitaires ciblées sur la base de l'analyse de leur panier. Le grand distributeur en question a pris connaissance de nos prises de position et a accepté de tenir compte de nos requêtes.

1.8.2 Contrôle dans le domaine des agences de renseignement économique et de renseignement en matière de crédit: Moneyhouse

Dans le cadre des recherches qu'elle propose sur des personnes, l'agence de renseignement économique Moneyhouse publie, entre autres, sur internet des données d'adresse que les personnes concernées avaient bloquées. Nous avons ouvert une procédure d'établissement des faits afin d'examiner de plus près les traitements de données en question.

Au début de l'été 2012, le nombre de questions émanant de particuliers et concernant le service en ligne Moneyhouse, géré par itonex SA, a brusquement augmenté. Les questions portaient en particulier sur la publication d'adresses par ailleurs bloquées, sur la présentation détaillée des réseaux sociaux des personnes concernées et sur la divulgation de données personnelles d'enfants mineurs. Ces données étaient publiées parmi les résultats de recherches sur internet. Des particuliers, qui ont tenté en vain d'entrer en contact avec Moneyhouse, se sont annoncés auprès de nos services. Ils désiraient que la publication de leurs données d'adresse soit interrompue le plus vite possible pour des raisons de sécurité. Nous avons donc par la suite ouvert une procédure d'établissement des faits.

Nous n'avons pas été plus chanceux dans la tentative d'entrer en contact avec l'agence en question que les citoyens susmentionnés. Nous avons donc requis l'ordonnance d'une mesure superprovisionnelle au Tribunal administratif fédéral (TAF). Notre but était que le service de recherche de personnes soit provisoirement suspendu du fait que la publication des adresses impliquait un risque majeur pour les personnes concernées.

Dans une première décision incidente, le TAF a enjoint Moneyhouse de suspendre provisoirement les recherches de personnes faisant l'objet de ces contestations. Dans une seconde décision incidente, le Tribunal a autorisé ultérieurement la fonction de recherche à des conditions strictes. Les données d'adresse doivent être effacées dans le délai d'un jour ouvrable si la personne concernée le demande.

Cette décision ne couvre pas la question de fond de savoir si la publication de données personnelles sur internet enfreint la protection des données.

Nous sommes d'avis que l'admissibilité de la publication sur internet de données d'adresse que les personnes concernées ont bloquées doit être examinée d'un point de vue juridique. Pour cette raison, nous avons concentré notre attention sur cette question dans la première partie de la procédure d'établissement des faits et établi également des recommandations à ce sujet, à l'intention de Moneyhouse. Cette agence spécialisée dans les renseignements économiques a accepté nos recommandations. Les autres traitements de données font actuellement l'objet de la deuxième partie de la procédure d'établissement des faits.

1.8.3 Envoi de pièces justificatives du registre du commerce par internet

L'été dernier deux cantons ont entamé une nouvelle pratique dans le cadre de la mise en œuvre du principe de la publicité de leurs registres du commerce. Ceux-ci transmettent désormais par courriel, instantanément, l'intégralité des pièces justificatives à toute personne qui en fait la requête. Cette transition inconditionnelle, d'une consultation qui nécessitait un déplacement au registre du commerce ou du moins un contact personnel à une publicité par le biais d'internet, soulève des questions essentielles relatives au droit de la protection des données et de la personnalité.

Les registres du commerce de Zurich et Bâle-Ville rendent leurs pièces justificatives accessibles par e-mail depuis le mois de juillet 2012. Notre attention a été attirée sur cet état de fait par des citoyens concernés ainsi que par les autorités de police. D'après les indications reçues, les documents mis à disposition du public par le biais d'une communication automatisée peuvent contenir des signatures, des dates de naissances, des adresses privées, des numéros de passeports, de cartes d'identité, de cartes de crédit et autres informations délicates du point de vue sécuritaire.

Le principe de publicité, ancré dans la loi, est indispensable au bon déroulement des affaires, certes. Cependant, les moyens utilisés à cette fin ne peuvent être affranchis de toute réflexion sur la protection des données. En effet, l'accès à de telles informations personnelles par un service en ligne pose problème et se traduit par des risques difficilement contrôlables (fraudes, falsifications de documents, assemblages de données, etc.). Pour les personnes concernées il s'agit de surcroît de la perte de la maîtrise sur leurs propres données et partant, sur leur droit

constitutionnel à l'autodétermination informationnelle. L'assemblage de données par des entreprises spécialisées dans la collecte et l'exploitation systématique de données personnelles, par exemple les sociétés de renseignement économique, s'en trouve facilitée. Ceux-ci les traitent ensuite pour en faire par exemple des profils de la personnalité à l'insu de l'individu intéressé. A cela s'ajoute l'élément international du problème: celui-ci n'est pas négligeable étant attendu que les données une fois publiées sur la toile ne connaissent pas de frontières. Les données sont, d'une part, soustraites au champ d'application du droit suisse et peuvent, d'autre part, être sujettes à un traitement dans des Etats qui ne connaissent pas de garanties équivalentes aux nôtres.

Du point de vue de notre activité de surveillance, il y a lieu de préciser, que nos moyens d'interventions sont limités dans le cas d'espèce. Notamment, car les registres publics relatifs aux rapports de droit privé sont expressément exclus du champ d'application de la loi fédérale sur la protection des données (LPD). Dans le cadre de nos attributions de conseil et d'assistance nous avons, cependant, initié une discussion avec l'Office fédéral du registre du commerce qui est l'autorité de surveillance compétente. Ceci, dans le dessein de le rendre attentif aux risques susmentionnés. Nous avons également pris position à plusieurs reprises dans le cadre des procédures de consultations lors de la révision du code des obligations et de l'ordonnance sur le registre du commerce, afin d'orienter le législateur sur les problèmes ressortissant à cet état de fait.

Au vu de ce qui précède, il sied d'attirer l'attention des personnes voulant procéder à une inscription dans ces cantons, devant le notaire déjà, sur les conséquences liées aux pratiques en vigueur à Zurich et Bâle-Ville. Ainsi, ils pourront faire usage des possibilités qui existent actuellement afin de limiter le contenu des pièces justificatives au strict nécessaire requis par la loi. Pour de plus amples informations concernant les modifications législatives en cours qui ont trait à ce sujet, voir ch. 1.8.4 du présent rapport d'activités.

1.8.4 Modernisation du registre du commerce – Modification du code des obligations

Le registre du commerce devant être modernisé, il est prévu de créer un fichier électronique central qui s'appuiera sur une infrastructure informatique unique. Du point de vue de la protection des données, nous sommes tout particulièrement favorables à l'introduction d'un droit à l'oubli.

Désormais, les inscriptions dans le registre du commerce seront directement intégrées sous forme électronique dans le fichier central et publié sur internet. L'index central des raisons de commerce (Zefix) deviendra donc superflu. En outre, le projet de loi contient une base légale permettant l'utilisation du numéro AVS dans le registre du commerce. Cela permettra une actualisation automatique des données et l'obligation de déclarer les changements de nom ou de nationalité disparaîtra. Le numéro AVS ne sera ni affiché ni publié. Nous avons toutefois souligné que le projet ne précisait pas avec suffisamment de détails les catégories de personnes qui auraient accès à ces numéros.

La réorganisation du registre du commerce simplifiera la collaboration entre les autorités. Ainsi, l'entraide administrative permettra de consulter dans le registre du commerce les inscriptions d'autres services sauf si des prescriptions en matière de protection du secret ne s'y opposent. En outre, un registre des personnes sera rattaché au registre du commerce: il permettra une meilleure identification. Le projet ne précisant pas les champs de données qui seront accessibles dans ce registre des personnes, nous avons donc attiré l'attention sur le fait que les organes de la Confédération ne doivent permettre l'accès en ligne des données personnelles sensibles que si celui-ci a fait l'objet d'une réglementation légale suffisante.

Dans le cadre de cette consultation des offices, nous avons de nouveau souligné les difficultés qu'entraîne la publication sans limite dans le temps de données du registre du commerce sur internet. Nous estimons depuis longtemps qu'il convient de peser les intérêts en présence sous l'angle temporel. L'intérêt public à la publication d'anciennes données économiques sur internet (par ex. les données sur une entreprise effacée après échéance du délai de prescription) devrait être examiné par rapport à l'intérêt particulier de la personne concernée à voir ces données retirées d'internet. Il existe d'autres canaux de publication qui correspondent mieux au principe de la proportionnalité qu'internet.

L'Office fédéral de la justice a accepté nos objections. Dans le projet qui a été mis au point suite à la consultation figure désormais un droit à l'oubli adapté au droit du registre du commerce. Nous approuvons cette adaptation et suivons avec intérêt les autres développements dans ce domaine. Pour de plus amples informations à ce sujet voir ch. 1.8.3 du présent rapport d'activités.

1.8.5 Traitement de données personnelles dans le commerce d'adresses

Nous avons pu clore sur de nombreux points l'examen des faits concernant un commerçant d'adresses. Seul le traitement des données concernant les avoirs immobiliers a dû faire l'objet d'une appréciation séparée. Nous sommes parvenus à la conclusion que ces données ne doivent être ni traitées, ni communiquées.

Au cours de l'exercice écoulé, nous avons poursuivi l'examen des faits à propos d'un commerçant d'adresses. Il est apparu, au cours de nos travaux et des entretiens avec les responsables, que ceux-ci faisaient preuve de compréhension, sur la majorité des points, concernant nos propositions d'amélioration en matière de protection des données. Presque toutes concernent, pour l'essentiel, les principes de la transparence et de l'information à propos de la collecte et du traitement des données. Ainsi, le commerçant d'adresses a accepté toutes nos propositions de modification conformément à notre rapport final. Le seul thème que nous avons dû aborder séparément a été le traitement des données concernant les biens immobiliers. Ces données comprennent par exemple l'année de construction du bâtiment, le nombre d'étages, mais aussi des informations extraites des demandes de permis de construire et autres détails concernant une adresse de domicile déterminée. Le commerçant d'adresses relie ces données avec les personnes habitant à l'adresse en question. Ces données constituent par conséquent des données personnelles au sens de la LPD. Les données sur les biens immobiliers proviennent en partie de sources publiques comme le registre foncier ou les demandes de permis de construire, mais leur publication dans ce cadre est en conformité avec le but poursuivi. Un traitement des données dans le domaine du commerce des adresses en vue d'activités de marketing ou d'autres affaires de tiers constitue par contre une violation du principe de la finalité de la LPD. Cette violation peut être légitimée par le consentement des personnes concernées, ce qui n'était toutefois pas le cas ici. Nous sommes donc parvenus à la conclusion que du fait de l'absence de motifs justificatifs, il fallait s'abstenir en l'espèce de traiter les données concernant les biens immobiliers. Le commerçant d'adresses en question a accepté cette exigence. Partant, il ne traitera ni ne transmettra

plus de données personnelles, dans ce cadre-là, en relation avec des personnes identifiables. Nous procéderons à un contrôle pour vérifier les détails de la mise en œuvre et nous nous prononcerons à ce sujet également.

1.8.6 Ouverture du marché de la poste: révision totale de l'ordonnance

Nous avons remis notre prise de position concernant la révision totale de l'ordonnance sur la poste dans le cadre de la consultation des offices. A cette occasion, nous nous sommes exprimés sur les devoirs d'information et sur la gestion des données d'adresses, notamment leur transmission à des tiers.

La révision totale de la loi sur la poste et de la loi sur l'organisation de la Poste, ainsi que les ordonnances correspondantes sont entrées vigueur au cours du dernier trimestre de l'année écoulée. Les lois avaient déjà été adoptées par le Parlement en 2010, mais il fallait encore réviser les ordonnances. Nous avons eu, dans le cadre de la consultation des offices, la possibilité de nous prononcer sur les projets d'ordonnance.

La révision totale de la législation sur la poste visait deux objectifs principaux: d'une part mettre en œuvre le mandat constitutionnel consistant à assurer le service universel par la fourniture de services postaux de paiement à l'ensemble de la population et, d'autre part, ouvrir complètement le marché postal pour les prestataires privés. La garantie de ce second objectif nécessite l'échange de données d'adresses. Lorsque nous avons examiné le projet d'ordonnance, nous avons concentré notre attention sur les devoirs d'information des prestataires de services au cours du traitement et de la transmission de données. En effet, un principe fondamental de la loi sur la protection des données est la transparence du traitement des données; les personnes ne peuvent faire valoir leurs droits que si cette transparence est garantie. La nouvelle législation oblige donc tous les fournisseurs de services postaux avec distribution à domicile qui participent à l'échange d'adresses d'informer leurs clients de leur mode de gestion des données d'adresses.

Si un fournisseur de services postaux désire transmettre des ensembles de données à des tiers, il doit demander pour cela l'autorisation des personnes concernées. Il ne suffit pas de mentionner, dans les conditions générales, l'intention de communiquer les données. En effet, ces personnes doivent être directement informées de la transmission de leurs données à des tiers, par exemple par courrier ou de manière visible sur les formulaires de mandats des clients. A cette occasion, il faut aussi

mentionner les catégories des destinataires de données, car les clients ne peuvent remettre une manifestation de volonté valable que s'ils savent exactement ce pour quoi ils donnent leur consentement. Ainsi, pour ces personnes, il est décisif de savoir si leurs données ne sont transmises qu'à des entreprises et des personnes avec lesquelles elles entretiennent une relation contractuelle directe (éditeurs de journaux, assurances, banques, etc.) ou aussi à des négociants d'adresses (prestataires d'adresses) et des sociétés de renseignements économiques.

Cette révision totale a aussi permis d'introduire une innovation importante. Effectivement, l'opposition à la transmission de ses données personnelles à des tiers ne doit avoir aucune suite financière. Une exigence de longue date du point de vue de la protection des données a ainsi été adoptée: le consentement doit être établi de manière libre et éclairé, à défaut de quoi il ne serait pas valable. Or, l'ancienne réglementation permettait de prélever un supplément auprès des clients de la poste qui s'opposaient à une transmission de leurs données à des tiers. Les réactions des citoyens au printemps lors de la dernière augmentation de cette taxe ont montré que le montant du supplément était susceptible d'avoir des répercussions sur la condition de liberté du consentement. Ce qui était problématique en ce sens que l'exercice d'un droit fondamental ne doit pas dépendre de considérations monétaires.

Les remarques que nous avons formulées dans le cadre de la consultation des offices à propos des devoirs d'information et de la gestion des données d'adresses, notamment sur la transmission de données personnelles à des tiers, ont donc été prises en compte. Les clients de la poste peuvent désormais se décider pour ou contre la transmission de leurs données d'adresses à des tiers sans répercussion financière.

1.8.7 Base de données d'un prestataire de services financiers en relation avec des évènements relevant de la sécurité

La collecte secrète de données relatives aux employés, aux clients et à des tiers par un prestataire de services financiers constitue une activité délicate du point de vue de la protection des données. Malgré les éventuelles obligations légales de diligence qui pourraient justifier une telle démarche, le traitement doit être conforme aux exigences et aux principes de la loi. Afin de clarifier cela, le PFPDT a ouvert une procédure d'établissement des faits en la cause.

Au cours de l'année écoulée, des informations parues dans la presse ont attiré notre attention sur une base de données soi-disant secrète et non conforme aux exigences de la protection des données, gérée par une grande banque suisse. Celle-ci contiendrait des données personnelles concernant des clients, des collaborateurs et des tiers, qui ont été en partie collectées à leur insu. Un examen des faits s'est avéré indispensable étant donné le haut potentiel d'atteinte à la personnalité d'un grand nombre de personnes.

Dans une première prise de position, la banque a argué que les données collectées sont nécessaires dans le cadre de l'évaluation sécuritaire de certains cas et que les traitements de données effectués sont justifiés par un intérêt prépondérant privé ainsi que par des obligations légales. La manière dont sont réglés les traitements, les accès, les flux de données, la durée de conservation et les conditions d'une communication fera l'objet de la procédure que nous avons entamé.

L'examen des faits est encore en cours.

1.9 International

1.9.1 Coopération internationale

L'année écoulée a été marquée par la poursuite des travaux de révision et de modernisation de la Convention 108, des lignes directrices de l'OCDE et du cadre juridique européen ainsi que par l'intensification des réflexions des commissaires à la protection des données en vue d'un renforcement de la coopération internationale. Nous avons participé à ces travaux et réflexions, notamment par une présence active au Conseil de l'Europe, à l'OCDE, aux conférences européenne et internationale des commissaires à la protection des données et au sein de l'Association francophone des autorités de protection des données. Nous avons également participé aux travaux des instances de contrôle commune Schengen, Eurodac et Visa.

Conseil de l'Europe

Le comité consultatif (T-PD) de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), présidé par le préposé fédéral suppléant, a poursuivi et achevé ses travaux en vue de la modernisation de cet instrument juridique contraignant. Il a ainsi adopté un projet d'amendement de la convention lors de sa 29e réunion plénière tenue à Strasbourg du 27 au 30 novembre 2012. Le projet sera transmis au comité des Ministres du Conseil de l'Europe qui chargera un comité ad hoc intergouvernemental de le finaliser. Ce comité devrait être ouvert à des Etats non membres du Conseil de l'Europe susceptibles d'adhérer à la Convention 108.

Les objectifs poursuivis par ces travaux de modernisation de la convention visent à répondre aux défis de l'utilisation des nouvelles technologies de l'information et des communications. Ils doivent permettre de renforcer le droit à la protection des données tout en le conciliant avec l'exercice d'autres droits et libertés fondamentales. Il s'agit également de renforcer les mécanismes de mise en œuvre et de suivi de la convention. Le texte doit respecter une approche technologiquement neutre et assurer la cohérence et la compatibilité avec le cadre de l'Union européenne. Enfin, ces travaux doivent contribuer à renforcer et à promouvoir la vocation universelle et le caractère ouvert de la convention.

L'objet et le but de la convention sont de garantir à toute personne physique le droit à la protection des données à caractère personnel afin d'assurer le respect des autres droits et libertés fondamentales lors du traitement de données à

caractère personnel. La convention révisée verra son champ d'application élargi à tout traitement de données personnelles quels que soient les moyens et procédés utilisés. Elle ne se limitera plus aux seuls traitements automatisés. Par contre et à juste titre, la convention sort de son champ d'application les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Par rapport au texte actuel, le projet de révision prévoit de préciser les contours du principe de la proportionnalité pour couvrir non seulement les données, mais également les traitements et le choix des moyens; il introduit d'autre part le principe de minimisation des données. Le projet définit également de manière générale les conditions de licéité du traitement, à savoir le consentement ou tout autre fondement légitime prévu par la loi. Cette dernière expression couvre notamment les motifs justificatifs énoncés à l'article 13 LPD et l'exigence de base légale pour les traitements des organes fédéraux au sens de l'article 17 LPD. Concernant les données sensibles, le principe de l'interdiction est maintenu. Ces données ne peuvent être traitées que lorsque le droit interne prévoit des garanties appropriées qui complètent les autres garanties énoncées dans la convention. Ces garanties supplémentaires doivent permettre de prévenir les risques que le traitement de données peut présenter pour la personne concernée. En outre, le catalogue des données sensibles est étendu aux données génétiques et aux données biométriques identifiant un individu de façon unique. Une distinction sera faite entre les données sensibles par nature, comme les données de santé et celle dont la sensibilité découle de l'usage qui en est fait, comme les données dont le traitement révèle l'origine raciale. Cette approche permet notamment qu'une photo ne soit pas automatiquement considérée comme une donnée sensible.

Le projet adopté par le T-PD prévoit également d'introduire une obligation d'annonce des violations de données lorsqu'elles sont susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées. L'annonce devrait être faite auprès des autorités de contrôle en matière de protection des données. Il n'est pas prévu d'informer les personnes concernées. Il reviendra cependant aux autorités de décider d'une telle information. Le projet introduit également une obligation d'informer les personnes concernées lors de la collecte de données personnelles. Il renforce également les droits des personnes concernées et précise les obligations au chef des responsables de traitement. En particulier, ceux-ci devront être capables de démontrer les mesures qu'ils prennent pour assurer la protection des données et devront procéder à des analyses d'impact. Les Parties à la convention devront en outre veiller à ce que les produits et les services destinés au traitement de données prennent en compte les implications du droit à la protection des données dès leur conception et facilitent

la conformité des traitements de données au regard du droit applicable («Privacy by design»).

En ce qui concerne les flux transfrontières, le projet maintient le principe de la libre circulation des informations entre les Parties. Toutefois, il préserve le régime spécifique mis en place au sein de l'Union européenne basée sur l'adéquation des Etats tiers. La reconnaissance de l'adéquation des Etats Parties non membres de l'Union européenne devrait cependant être facilitée. Le transfert vers des Etats tiers repose sur l'exigence d'un niveau approprié de protection des données qui peut être garanti par des dispositions légales ou reposer sur des garanties ad hoc ou standardisées prévues dans des instruments juridiques contraignants (par exemple contrats ou règles d'entreprises contraignantes). La communication en l'absence d'un niveau approprié demeure possible avec le consentement, lorsqu'elle est nécessaire pour protéger des intérêts spécifiques de la personne concernée ou pour remplir des intérêts légitimes prépondérants, notamment des intérêts publics importants prévus par la loi. Des dérogations sont aussi possible pour garantir la liberté d'expression et d'information. Les autorités de protection des données doivent cependant avoir un droit d'intervention, notamment en relation avec les garanties ad hoc.

Le projet de révision renforce également les compétences des autorités de contrôle. Celles-ci se verront attribuer des compétences de décisions et de sanctions. Leur indépendance devrait être mieux garantie. Elles doivent en particulier être dotées de ressources humaines, techniques et financières adéquates et disposer des infrastructures nécessaires pour accomplir leurs tâches et exercer leurs pouvoirs de manière indépendante et effective. Enfin, la coopération entre autorités de protection des données doit être renforcée, notamment en vue de coordonner leurs interventions et leurs investigations ou en menant des actions conjointes.

L'un des défauts de la convention actuelle est d'une part l'absence de contrôle préalable à la ratification ou à l'adhésion et d'autre part l'absence de suivi du respect des obligations qui en découlent. Le projet prévoit que les Parties devront prendre dans leur droit interne les mesures nécessaires pour donner effet aux dispositions de la présente Convention et assurer leur application effective. Ces mesures devront être prises préalablement à la ratification ou à l'adhésion. En outre, les Parties devront permettre au Comité conventionnel d'évaluer le respect de leurs engagements. Le Comité conventionnel voit ainsi son rôle renforcer. Outre les fonctions consultatives actuelles, il pourra évaluer la conformité du niveau de protection des données d'un Etat avec les dispositions de la Convention et examiner périodiquement l'application de la Convention par les Parties.

Le PFPDT soutient le projet adopté par le comité consultatif. Ce projet une fois adopté par le comité des Ministres nécessitera une modification de nos législations fédérales et cantonales en matière de protection des données.

Conférence européenne des commissaires à la protection des données

La conférence européenne de printemps des commissaires à la protection des données s'est déroulée à Luxembourg du 3 au 4 mai 2012 et a été organisée par la commission luxembourgeoise de la protection des données. La conférence réunissait des délégués des autorités de protection des données de 38 pays, ainsi que des représentants du Conseil de l'Europe, des instances européennes et de l'OCDE. Intitulée «réforme de la protection des données européenne confrontée aux attentes!», la conférence a débattu des projets de réforme de l'Union européenne et de la modernisation de la Convention 108. Nous avons eu ainsi l'occasion de présenter les travaux de révision de la Convention 108 (voir Conseil de l'Europe ci-dessus). Ces réformes tendent à rendre les législations de protection des données plus efficientes et plus claires non seulement pour ceux et celles qui traitent des données, mais également pour les individus de façon à leur conférer davantage de transparence et de maîtrise sur leurs données et leur faciliter l'exercice de leurs droits. Les commissaires ont ainsi débattu du renforcement des droits des utilisateurs de services internet, de la nécessité de simplifier les obligations administratives des différents acteurs au profit d'une plus grande responsabilisation, de l'évolution et du renforcement du rôle des autorités de protection des données. Concernant le rôle des autorités de protection des données, la vice-présidente de la Commission européenne, Viviane Reding, commissaire européenne à la justice a relevé que «la réforme de la protection des données, présentée par la Commission européenne, établit un seul et même ensemble de règles de protection des données fortes qui assurent davantage de contrôle sur leurs données à nos citoyens tout en rendant plus aisé aux entreprises d'être en conformité pour tirer profit du Marché unique. Mais une législation uniforme, ce n'est pas suffisant. Nous avons aussi besoin que quelqu'un veille à ce que ces règles soient appliquées partout à travers l'UE, et partout de la même façon. C'est pour cela que notre réforme renforce considérablement le rôle des autorités de contrôle national et harmonise leurs missions et pouvoirs de façon à ce qu'elles puissent faire de ces règles une réalité effective pour les citoyens européens et les entreprises.»

Les commissaires ont adopté une résolution relative à la réforme européenne de la protection des données dans laquelle ils relèvent et reconnaissent les efforts

entrepris pour renforcer les droits des individus et améliorer leur effectivité en tenant compte des changements technologiques et de la globalisation. Les commissaires saluent en particulier l'intention de renforcer la responsabilité des différents acteurs impliqués et notamment des responsables de traitement, la volonté de diminuer les charges administratives, ainsi que l'intention d'améliorer la cohérence du cadre juridique et de renforcer le rôle des autorités de protection des données. Ils attirent néanmoins l'attention sur le risque d'avoir différents régimes de protection des données au travers d'exceptions et de dérogations au cadre général de protection des données. Ils souhaitent en particulier que le niveau de protection des données dans le secteur de la police et de la coopération judiciaire en matière pénale soit aussi élevé que pour les secteurs régis par le projet de règlement général.

La résolution se trouve sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale

Autorité de contrôle commune Schengen

L'autorité de contrôle commune Schengen (ACC) s'est réunie à quatre reprises en 2012. Elle a élu à sa présidence, le préposé fédéral suppléant. L'ACC a poursuivi ses activités de contrôle, notamment son inspection sur les alertes relatives aux personnes recherchées pour l'arrestation aux fins d'extradition. Le rapport final et les recommandations qui l'accompagnent seront adoptés au premier trimestre 2013. Elle a finalisé son rapport concernant le suivi des recommandations adoptées à l'issu de l'inspection relative aux données de personnes ou de véhicules intégrées dans le SIS aux fins de surveillance discrète ou de contrôle spécifique. Ce rapport sera publié. Une enquête relative à l'exercice du droit d'accès dans les différents Etats Schengen est également en cours et devrait être achevée en 2013. L'ACC a également pris connaissance des contrôles effectués par le PFPDT dans les ambassades suisses hors de la zone Schengen et souligné l'importance de mener de tels contrôles. L'ACC suit en outre les développements relatifs au SIS2 et notamment la migration du SIS1+ vers le SIS2 qui devrait débutée au premier trimestre 2013. Elle souhaite en particulier être impliquée dans la mise en place de la nouvelle structure de contrôle prévue par la réglementation du SIS2.

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 d'informer les cantons sur les développements en cours et sur les activités de l'ACC, de planifier des activités de contrôle et d'échanger des informations.

En 2012, le groupe a notamment eu l'occasion d'échanger leurs idées sur les méthodes de contrôle.

Groupe de coordination du contrôle d'Eurodac et de VIS

Nous avons participé aux réunions du groupe de coordination Eurodac qui ont eu lieu le 24 mai et le 21 novembre 2012. Le Contrôleur Européen de la protection des données (CEPD) a à cette occasion informé sur le contrôle effectué auprès de l'unité centrale d'Eurodac. Un autre sujet également abordé a été le contrôle coordonné des empreintes digitales illisibles. Ont également été discutés le questionnaire pour le contrôle des organes responsables dans les divers Etats membres de communiquer avec l'unité centrale ainsi que le projet de refonte du règlement Eurodac de la Commission européenne. Un autre point de discussion a été le transfert des données Eurodac de la Commission Européenne à l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle. L'agence a son siège à Tallinn en Estonie et le serveur se trouve à Strasbourg (France).

Le 21 novembre 2012 a eu lieu la première réunion officielle du groupe de coordination du VIS. Comme mentionné dans notre dernier rapport d'activités, le système d'information sur les visas (VIS) a pu être mis en œuvre pour la première région le 11 octobre 2011 (voir notre 19e rapport d'activités 2011/2012, ch. 1.10.1). Le groupe de coordination du VIS est constitué de la même manière que celui chargé du contrôle d'Eurodac et se compose également du CEPD et des autorités nationales de protection des données. C'est la raison pour laquelle nous y sommes aussi représentés. Parmi les points traités, la question de la mise en service du VIS le 2 octobre 2012 pour une autre région, à savoir les Etats du Golfe. Le CEPD a en outre fait état de l'inspection qu'il a effectuée auprès de la centrale du VIS.

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

La 34e Conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue à Puenta del Este en Uruguay du 23 au 26 octobre 2012 (www.privacyconference2012.org). Comme à l'accoutumé, la conférence réunissait des autorités de protection des données issues des 4 continents, des représentants de l'industrie et de la société civile, des délégués gouvernementaux, des organisations internationales et des académiciens. Elle était divisée en deux parties, l'une réservée aux autorités de protection des données et l'autre ouverte aux autres acteurs intéressés. Le programme de la 34e Conférence s'articulait autour du thème «Vie privée et technologie en équilibre». Elle a permis une réflexion globale

sur les attentes de la société de l'information eu égard aux standards et règles de protection des données personnelles. Elle a également examiné différentes stratégies mises en place par les Etats dans le cadre de la société d'information en vue notamment de développer un mode de gouvernement, plus efficace, plus transparent, qui repose sur l'utilisation des nouvelles technologies. Il s'agissait en particulier de réfléchir au cadre juridique de l'administration en ligne. La conférence a également fait le point sur les différents modèles juridiques existants ou en préparation en matière de protection des données et de la vie privée. L'aspect des technologies et de leur impact sur la protection des données (géolocalisation, biométrie, données intelligentes) ainsi que les défis pour la protection des données découlant de certaines applications technologiques (publicité comportementale en ligne, gouvernement transparent) ont également été abordés. De même, la conférence a abordé quelques aspects spécifiques du droit de la protection des données et notamment le consentement éclairé, la protection des données de santé, la lutte contre le piratage ou la coopération internationale des autorités de protection des données.

Lors de la conférence réservée aux autorités de protection des données, les commissaires ont eu l'occasion d'approfondir la question de l'amélioration de la coopération internationale et de la structuration de la conférence. Ils ont également eu un large échange de vue sur la question du profilage. Les commissaires ont en outre adopté une résolution sur l'avenir de la vie privée. Dans cette résolution, ils s'engagent à intensifier la coopération mutuelle afin de répondre de manière coordonnée, notamment par des actions conjointes, aux défis transfrontières pour la protection des données et aux risques pour la vie privée. Ils s'engagent également à échanger des informations et à partager des expériences afin d'optimiser leurs ressources. Ils veilleront à promouvoir une meilleure interopérabilité entre les différents systèmes juridiques et régimes de protection de la vie privée. Les commissaires ont également adopté une résolution dans laquelle ils recommandent en particulier que l'infonuagique n'aboutisse pas à un affaiblissement des standards de la protection des données. Les responsables de traitement sont ainsi invités à procéder à des analyses d'impact de la vie privée avant de recourir à l'infonuage. Les fournisseurs de services dans l'infonuage doivent en assurer la transparence et offrir des garanties de sécurité suffisante; ils doivent en particulier pouvoir annoncer les violations de données et permettre aux utilisateurs de garder le contrôle des données. Le recours aux technologies de la vie privée (privacy by design) et à la certification doit être encouragé. Enfin, la conférence a adopté une déclaration finale relative au profilage. Le recours à ces techniques se doit d'être conforme aux exigences de protection des

données (notamment transparence, respect de la proportionnalité, évaluation des algorithmes utilisés dans les activités de profilage, intervention humaine dans les opérations de profilage, contrôle par des autorités indépendantes).

Les résolutions et la déclaration finale se trouvent sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale.

(infonuagique = cloud computing; infonuage = cloud)

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

Au cours de l'exercice 2012, ce groupe de travail s'est consacré en particulier à la révision des directives relatives à la sécurité et à la protection des données. Les directives sur la sécurité des réseaux d'information sont aussi en réexamen. Enfin, le groupe de travail s'est penché sur la question du caractère économique des informations personnelles en relation avec la protection des données et la sécurité.

Le groupe d'experts constitué en vue de la révision des directives relatives à la sécurité et à la protection des données a établi la méthodologie et le cadre du processus de révision dans un document, lequel a été adopté au terme d'une phase de consultation. Ce groupe n'avait pas comme objectif premier de tout modifier, mais de moderniser les directives tout en conservant certains principes, encore valables même à l'ère d'internet. A ce propos, des commentaires explicatifs supplémentaires tenant compte des données techniques actuelles devraient encore être rédigés. Au terme d'intenses discussions entre le groupe d'experts et le groupe de travail, des propositions de révision ont été présentées. Les huit principes fondamentaux de ces directives ont été conservés, car ils sont toujours d'actualité. Par contre, les directives ont été complétées dans le but de garantir une protection des données plus efficace.

Outre de petites modifications d'ordre rédactionnel, l'introduction de programmes de gestion de la sphère privée est un point déterminant. Ils ne sont pas encore définis d'un point de vue juridiques, mais ils imposeront probablement aux maîtres de fichiers des obligations supplémentaires. Il faut considérer ces programmes en quelque sorte comme un règlement de traitement élargi, applicable à tous les traitements de données du maître du fichier. Les principaux aspects en sont: l'inventaire de toutes les mesures de protection et de sécurité des données, la mise œuvre de mesures prônant le respect de la vie privée dès la conception et le fonctionnement des systèmes et des réseaux informatiques («privacy by design»), l'architecture des systèmes, le rôle du conseiller à la protection des données et,

enfin, le traitement des problèmes de protection et de sécurité des données. En outre, les propriétaires de fichiers devraient être tenus de présenter sur demande aux autorités de protection des données leurs programmes de gestion de la sphère privée.

En cas de violation de la sécurité des données ou de la protection des données, il est également prévu que le propriétaire du fichier soit tenu d'en informer les autorités et le public. Une autre modification concerne la désignation d'autorités de protection des données, indépendantes et dotées de suffisamment de moyens techniques. A propos de la transmission de données personnelles vers l'étranger, l'accent est mis sur la nécessité de modèles adéquats qui garantissent la protection des données au-delà des frontières nationales. Il est fait référence à ce propos au modèle, applicable en Suisse et dans l'Union européenne, de la «liste des Etats» possédant une législation assurant un niveau de protection des données de même valeur.

D'autres modifications concernent le renforcement de la coopération internationale, la sensibilisation et la formation, les mesures techniques favorisant une plus grande protection des données («privacy enhancing technologies») et la garantie d'une protection des données transfrontalière, quel que soit l'endroit où les données se trouvent. Autrement dit, il ne doit plus être possible de contourner les dispositions légales en matière de protection des données en choisissant un pays déterminé pour stocker ses données. Enfin, les directives établiront expressément que la protection des données personnelles est un droit fondamental.

Un document supplémentaire rassemble toutes les propositions qui n'ont pas été entièrement prises en compte dans le processus de révision, mais qui doivent être débattues prochainement. Cela concerne en particulier l'impératif de l'information et du consentement («notice and choice»), ainsi que la nécessité de limiter l'utilisation des données personnelles («specification and use limitation»). Les commentaires d'origine sur la directive demeurent, alors que les nouveautés (modifications et compléments) seront répertoriées dans un document supplémentaire, déclarés comme tel. Ainsi deux commentaires explicatifs accompagneront les directives et en feront partie intégrante.

Si l'on considère qu'à l'intérieur de l'OCDE, plusieurs systèmes juridiques doivent être pris en compte, les modifications proposées sont certainement un pas dans la bonne direction pour la Suisse et l'espace européen au sens large. Néanmoins, cette révision ne permettra très probablement pas de tenir compte de tous les principes de protection de données connus en Europe. Elle devrait être achevée au cours de la seconde moitié de l'année 2013.

Parallèlement, les directives concernant la sécurité des réseaux d'information est aussi en cours de révision: leur contenu fondamental ne doit certes pas être modifié, mais il va falloir les adapter aux données et aux nécessités techniques actuelles. Il faut en particulier y intégrer les questions de sécurité concernant les infrastructures informatiques critiques en relation avec internet. Le point essentiel est le partage de la responsabilité entre l'Etat et le secteur privé lorsqu'il s'agit de sécurité. Les directives de sécurité ne seront pas unies aux directives en matière de protection des données, mais il convient de mettre en évidence les synergies, par exemple par un référencement des dispositions y relatives.

À propos de l'étude du caractère économique des informations personnelles en relation avec la protection des données et la sécurité, quatre domaines ont été choisis au cours des séances de l'exercice précédent (réseaux sociaux, agences de renseignement commercial, moteurs de recherche et programmes de fidélisation de la clientèle) sur la base desquels des calculs ont été effectués. Divers résultats sont à relever, par exemple à propos des prix que les entreprises offrent pour des ensembles de données, mais aussi de ceux pratiqués sur les marchés illégaux. D'autre part, les prix diffèrent grandement de la valeur que les personnes concernées indiquent pour les différents ensembles de données (autoévaluation) et du prix largement plus bas que les individus seraient prêts à payer pour leur protection. Ces valeurs sont différentes selon les Etats, en fonction de la perception locale de la sphère privée. Nous citerons comme exemple les conceptions divergentes entre les citoyens européens et les citoyens des Etats-Unis ainsi que celles des citoyens en Asie.

Cette étude est terminée. Elle indique les différentes possibilités qui existent pour calculer la valeur ou le prix des ensembles de données.

Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP) a tenu sa sixième conférence et son Assemblée générale du 21 au 23 novembre 2012 à Monaco. La conférence a débuté par un volet réservé aux représentants des Etats et des autorités francophones du continent africain. Ce volet a permis aux autorités de ces Etats d'aborder les enjeux de la protection des données personnelles et de proposer des réponses spécifiques au continent africain.

Les discussions ont porté sur les instruments juridiques en cours d'élaboration, sur les enjeux de la biométrie en matière de protection des données et sur le gouvernement transparent (open data), ainsi que les difficultés rencontrées dans la mise en place des nouvelles autorités de protection des données et au développement d'une culture «protection des données». Le second volet de la

conférence a permis de mettre en valeur les travaux et les positions des autorités francophones. Les autorités ont abordé la question du contrôle par les autorités de protection des données du développement de l'administration électronique, les tâches de sensibilisation des autorités de protection des données, l'éducation numérique avec notamment la présentation de la plateforme www.thinkdata.ch, le recours à la biométrie lors des élections et l'importance pour les autorités de protection des données de disposer d'une expertise technique dans le cadre de l'exercice de leurs compétences. Lors des discussions relatives au recours à la biométrie dans le cadre des élections en Afrique, notamment pour éviter les fraudes (votes multiples), nous avons constaté que le recours à la biométrie est loin d'atteindre les objectifs recherchés et répond plus à des objectifs commerciaux de certaines entreprises européennes. En effet, la biométrie ne permet pas de résoudre les problèmes de dysfonctionnement notamment au niveau des registres de population dans les pays concernés. Il est également à relever que la présentation de la plateforme thinkdata a suscité un grand intérêt auprès de plusieurs autorités francophones qui pourraient s'approprier ce service dans le cadre de leurs activités de sensibilisation. Enfin, les participants ont manifesté leur souhait que les compétences technologiques des différentes autorités soient mises en réseau.

Lors de son Assemblée générale, l'AFAPDP a pris connaissance d'un rapport intermédiaire sur la mise en place d'un cadre permettant d'apprécier dans la pratique le caractère adéquat de la protection apportée aux transferts de données (notamment établissement de clause contraignante d'entreprise). Ce cadre devrait être adopté dans le courant 2013. L'Assemblée a pris connaissance de l'état d'avancement des travaux relatifs à la modernisation de la Convention 108. Elle a adopté une déclaration soutenant l'adoption d'un instrument mondial de protection des données personnelles inspiré des standards internationaux adoptés à Madrid en 2009 (voir 17e Rapport d'activités 2009/2010, ch. 1.10.1). Il s'agit d'un objectif à long terme qui passe par des étapes intermédiaires, dont l'adhésion d'Etats non membres du Conseil de l'Europe à la Convention 108. L'AFAPDP pourrait à l'avenir jouer également un rôle dans la promotion de la convention auprès des Etats émergents. Cette dernière devient ainsi un partenaire influent sur la scène internationale de la protection des données, non seulement par le soutien qu'elle apporte, avec l'aide de l'Organisation internationale de la francophonie, aux Etats émergents, mais également par sa participation active dans les débats mondiaux. Elle a ainsi le statut d'observateur au Conseil de l'Europe et au sein de la Conférence internationale des commissaires à la protection des données.

La déclaration de Monaco se trouve sur notre site www.leprepose.ch, sous Le PFPDT – Coopération internationale

2. Principe de la transparence

En 2012, le nombre de demandes d'accès a augmenté de plus de 8% par rapport à l'exercice précédent. Le pourcentage des accès complets et des refus complets est par contre demeuré stable. On enregistre une légère diminution de 3% des accès partiels (y compris les accès accordés au terme d'un certain laps de temps). La plus grande surprise cette année vient de la baisse massive des émoluments facturés. Enfin, le nombre de demandes en médiation déposées a augmenté de 20%, il y en a eu 78.

2.1 Demandes d'accès

2.1.1 Départements et offices fédéraux

Selon les chiffres qui nous ont été communiqués, 506 demandes d'accès ont été déposées auprès des autorités fédérales en 2012. Dans 223 cas, les autorités ont accordé un accès complet et dans 120 cas un accès partiel. Dans 138 cas, l'accès aux documents a été totalement refusé. 19 demandes d'accès ont été retirées; dans plus de la moitié des cas le retrait a été motivé par le montant des émoluments requis par les autorités. En 2012 six cas étaient encore en suspens. Il est à noter que le nombre de demandes d'accès déposées auprès des autorités ne cesse d'augmenter. Toutefois, la répartition proportionnelle des accès complets, des refus complets ainsi que l'octroi partiel des accès est demeurée très stable (cf. Statistique ch. 3.7 du présent rapport d'activités). L'augmentation générale des demandes d'accès, en tant que moyen, pour les citoyens, d'obtenir des informations, est certainement due à la notoriété croissante de la loi sur la transparence. La loi sur la transparence est désormais en vigueur depuis six ans. La stabilisation du nombre d'accès accordés et d'accès refusés témoigne de la sensibilisation des autorités à ce propos. L'apparition d'une certaine habitude, accompagnée d'une systématique dans le traitement des demandes d'accès y est également pour quelque chose. On ne relève aucun changement par rapport à l'année précédente pour ce qui est du pourcentage des refus complets (27%) et des accès complets (44%).

C'est la COMCO qui nous a transmis le plus grand nombre de demandes d'accès pour l'année 2012 (27 demandes), suivi de l'OFEV (25), de l'OFSP (24) et de l'ODM (23). Parmi les départements, le DETEC (100), le DFAE (88) et le DFE (80; depuis le 1er janvier 2013 Département fédéral de l'économie, de la formation et de la recherche DEFR) sont en tête. Sur 72 autorités, 16 nous ont informés qu'elles n'avaient reçu aucune demande d'accès pour l'année 2012. L'évolution constatée au cours

de l'année précédente, à savoir que les autorités demandent plus souvent des émoluments, (possibilité prévue d'ailleurs dans la loi sur la transparence), ne s'est pas poursuivie en 2012, au contraire: cette tendance à l'augmentation constante, dans certains cas massive, des émoluments a véritablement diminué. Seuls cinq instances administratives en ont prélevés en 2012, pour la somme de 6300.00 francs, soit la moitié par rapport à l'année précédente.

En ce qui concerne la charge de travail occasionnée par les demandes d'accès, nous rendons attentif au 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 continué d'augmenter (2010: 815 heures; 2011: 1519 heures; 2012: 2155 heures). Les heures consacrées à la participation à des procédures de médiation a légèrement augmenté pour passer de 453 heures en 2011 à 480 heures en 2012.

2.1.2 Services parlementaires

Les Services parlementaires nous ont informés qu'ils n'ont reçu aucune demande en 2012.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a informés avoir reçu quatre demandes d'accès pour l'année 2012: il a accordé un accès complet, un accès partiel et un refus complet. Seul un accès a été reporté dans le temps.

2.2 Demandes en médiation

En 2012, nous avons reçu un total de 78 demandes en médiation (cf. statistique ch. 3.10 du présent rapport d'activités), ce qui représente une augmentation d'exactement un cinquième par rapport à la période précédente (65 demandes). La plupart d'entre elles ont été déposées par des journalistes (33 demandes), suivis par les particuliers (21). D'une manière générale, les particuliers ont avantage fait usage de la possibilité de déposer une demande en médiation. Ces chiffres permettent de faire les remarques suivantes: sur un total de 258 cas, l'administration fédérale a refusé l'accès complètement 138 fois et l'a accordé partiellement 120 fois. Suite à ces refus complets et partiels, 78 demandes en médiation ont été déposées chez nous. Cela signifie qu'à peine 30 % des accès entièrement ou partiellement refusés, ont par la suite été suivis d'une demande en médiation.

Au total, 61 demandes en médiation ont été menées à terme durant l'exercice 2012. Parmi celles-ci, 20 avaient été déposées au cours de la même année, 35 dataient de l'exercice 2011 et six de l'exercice 2010. Dans six cas, nous avons pu trouver une solution consensuelle avec les parties impliquées. Nous avons émis des recommandations dans 19 cas faute d'avoir pu parvenir à une solution. Ainsi 26 demandes ont pu être réglées en médiation. Dans trois cas, l'autorité a accordé d'elle-même l'accès demandé en cours de procédure de médiation. Seize demandes ont été retirées et dans quatorze cas, les conditions d'application de la loi sur la transparence n'étaient pas données. Dans trois cas, la demande en médiation n'a pas été remise dans les délais. Dans dix cas sur 25, les procédures en médiation ont été menées à terme avec une médiation ou une recommandation et nous avons réussi à obtenir une solution plus favorable pour le requérant (à savoir une médiation ou un accès plus étendu que celui qui avait été accordé à l'origine par les autorités).

En raison de l'augmentation du nombre de demandes, les requérants continuent d'attendre plus longtemps que les 30 jours prévus par la loi le moment de la tenue de la procédure requise. Ceci est dû au fait que les ressources du Service en matière de personnel demeurent limitées.

2.3 Procédures de médiation closes

2.3.1 Recommandations

Les recommandations émises au cours de l'exercice 2012 concernant la loi sur la transparence sont brièvement résumées ci-dessous. Ces recommandations peuvent être consultées dans leur version intégrale sur notre site internet www.leprepose.ch, sous la rubrique Principe de la transparence – Recommandations – 2012.

Recommandation MPC / Contrat de travail de l'ancien procureur de la Confédération (22 février 2012)

Le demandeur a requis l'accès au contrat de travail que le Ministère public de la Confédération (MPC) avait conclu avec l'ancien procureur de la Confédération Erwin Beyeler pour la période allant de janvier 2012 à février 2012. Le MPC a répondu par la négative, arguant du fait qu'il était exclu du champ d'application de la loi sur la transparence depuis le 1er janvier 2011. Il estime en outre que l'accès au document en question devait de toute manière être refusé dans le but de protéger la sphère privée de Monsieur Beyeler. En revanche, dans sa recommandation, le Préposé à la protection des données et à la transparence a conclu que la loi sur la transparence était applicable dans le cas d'espèce et qu'il existait un intérêt public prépondérant à la consultation du contrat de travail de l'ancien Procureur de la Confédération Beyeler; sa sphère privée ne serait que légèrement touchée – si tant est qu'elle le soit – par l'accès à ce document.

Recommandation SECO / Listes d'entreprises Contrat collectif de travail (3 avril 2012)

Après la décision du Conseil fédéral d'étendre le champ d'application d'une convention collective de travail (CCT), plusieurs demandeurs ont requis auprès du Secrétariat d'Etat à l'économie (SECO) l'accès à des listes qui avaient été prétendument remises au SECO par une Commission paritaire nationale. Le SECO a confié aux demandeurs une partie de ces listes en précisant qu'il ne possédait pas d'autres documents. Le Préposé est de ce fait parvenu à la conclusion que la loi sur la transparence n'était pas applicable.

Recommandation OFSP / Liste des mesures des teneurs en acrylamide (19 juin 2012)

Le demandeur a requis de l'Office fédéral de la santé (OFSP) l'accès à un tableau de données que le Laboratoire cantonal de Zurich avait établi sur mandat de l'OFSP dans le but d'enquêter sur les teneurs en acrylamide de produits alimentaires. L'OFSP a refusé cet accès dans sa totalité, arguant que le rapport «Acrylamide monitoring in Switzerland, 2007-2009: results and conclusions» répondait au besoin d'information du public. Il invoquait en outre le fait que l'accès à cette liste impliquerait la publication de secrets d'affaires et de fabrication. Dans sa recommandation, le Préposé a constaté que le droit d'accès subjectif du demandeur n'était pas respecté par la publication scientifique d'un journal en ligne; la LTrans requiert la publication par la Confédération sur papier ou sous forme électronique sur le site de la Confédération. Il a en outre estimé que la liste ne contenait ni secrets d'affaires, ni secrets de fabrication. Il a de ce fait recommandé la mise à disposition de la liste sous forme anonymisée.

Recommandation OFSP / Annexe au protocole de la Commission fédérale des médicaments (25 juin 2012)

Le demandeur a requis de l'Office fédéral de la santé publique (OFSP) de pouvoir accéder aux annexes au protocole (les résumés) de la Commission fédérale des médicaments qui conseille l'OFSP dans l'élaboration des listes dite des spécialités. L'Office a refusé en partie l'accès à ces résumés, en invoquant le fait que certains documents constituaient les fondements d'une décision administrative encore en suspens. Par ailleurs, il estimait que ces résumés contenaient des secrets d'affaires et de fabrication ainsi que des données personnelles qui ne devaient pas être divulguées. Dans sa recommandation, le Préposé a conclu que l'office avait refusé l'accès à juste titre, d'une part parce que dans certains cas, la décision administrative n'avait pas encore été rendue, d'autre part parce que les résumés renfermaient effectivement des secrets d'affaires et de fabrication dignes de protection, ainsi que des données personnelles.

Recommandation EPFZ / Documents contractuels (16 juillet 2012)

Le demandeur a requis de l'Ecole polytechnique fédérale de Zurich (EPFZ) l'accès à des documents (environ 600 pages) concernant le contrat de développement d'un programme informatique que l'école avait conclu avec une entreprise. L'EPFZ a rejeté la demande dans son intégralité et précisé à ce propos que les documents renfermaient des secrets d'affaires et de fabrication et qu'en outre, leur publication violerait le droit de la protection des données ainsi que les droits de la personnalité des collaborateurs de l'EPFZ. Dans sa recommandation, le Préposé a relevé en

premier lieu que le fardeau de la preuve revient aux autorités quant à la présence d'un motif exceptionnel et que de ce fait, une limitation de l'accès sans raison valable n'était pas légale. En second lieu, il a estimé que les autorités doivent toujours tenir compte du principe de la proportionnalité lorsqu'elles examinent des demandes, raison pour laquelle l'accès aux passages qui ne sont pas couverts par une clause d'exception de la loi sur la transparence doit obligatoirement être accordé. Etant donné la multitude des documents que le demandeur désirait consulter, le Préposé a recommandé à l'EPFZ de remettre au demandeur une liste des documents important afin que celui-ci puisse préciser sa demande d'accès.

Recommandation ChF / Chronologie de la démission de Philipp Hildebrand (20 juillet 2012)

Le demandeur a requis de la Chancellerie fédérale (ChF) de pouvoir accéder à la chronologie de la démission du président de la Banque nationale suisse. La ChF a refusé cet accès, motivant sa décision entre autres par le fait que les documents destinés au Conseil fédéral n'étaient pas publiés. Dans sa recommandation, le Préposé a précisé que la ChF, en qualité d'état-major du Conseil fédéral, avait établi cette chronologie à titre de note d'information directement sur le mandat du Conseil fédéral. De ce fait, la propriété de la note d'information était attribuée au Conseil fédéral. Etant donné que le champ d'application de la loi sur la transparence ne s'étend pas au Conseil fédéral, le Préposé a recommandé à la ChF de maintenir sa décision et de ne pas transmettre les documents en question.

Recommandation OFL / Vente SWAG (9 août 2012)

Le demandeur a requis de l'Office fédéral du logement (OFL) l'accès à tous les documents concernant la vente de la Sapomp Wohnbau SA (SWAG) par la Confédération. L'OFL avait chargé une entreprise privée pour s'occuper de la vente. L'office a reconnu l'applicabilité de la loi sur la transparence et s'est prononcé en faveur de l'accès partiel aux documents; il a de ce fait nié l'existence de secrets d'affaires et approuvé la communication de données en raison de la présence d'un intérêt public prépondérant. Il a de surcroît refusé l'accès à certains documents sur la base des exceptions prévues dans la loi sur la transparence ainsi que sur la base du fait que les documents contiennent des données personnelles de tiers. En outre, l'OFL a mentionné le fait qu'une partie des documents demandés ne se trouvaient pas en sa possession. Dans ce cas concret il a estimé que la direction du Département avait pris sa décision définitive concernant la vente de la SWAG sur la base des documents qui lui avaient été remis par l'OFL et que l'OFL avait auparavant reçu ou requis de l'entreprise mandatée tous les documents importants. Pour sa part, le Préposé a aussi nié la présence de secrets d'affaires,

mais a reconnu la présence d'un intérêt public prépondérant à l'accès à certaines données personnelles. D'une manière générale, le Préposé a donc recommandé l'accès à la majorité des documents.

Recommandation OFAS / Procès-verbaux de séances de la Commission fédérale de l'AVS/AI (16 août 2012)

Le demandeur a requis de l'Office fédéral des assurances sociales (OFAS) l'accès aux procès-verbaux de séances de la Commission fédérale de l'AVS/AI des années 2011 et 2012. L'OFAS a refusé l'accès à ces documents en alléguant que ladite commission, en sa qualité de commission administrative, ne relevait pas du champ d'application de la loi sur la transparence et qu'en outre, ses séances étaient confidentielles conformément à son règlement interne. Dans sa recommandation, le Préposé a renvoyé à des jugements rendus par le Tribunal administratif fédéral le 17 juin 2011 et le 7 décembre 2011 (cf. notre 19e rapport d'activités 2011/2012 ch. 2.4) conformément auxquels la commission administrative faisait également partie, au plus tard depuis le 1er janvier 2009, de l'administration fédérale décentralisée et que de ce fait, elle entrait dans le champ d'application de la loi sur la transparence. Etant donné que l'OFAS ne pouvait présenter aucun motif d'exception, le Préposé a recommandé d'accorder l'accès aux procès-verbaux de séances.

Recommandation SECO / Modification de l'extension du champ d'application de la CCT (18 septembre 2012)

Le demandeur a requis du Secrétariat d'Etat à l'économie (SECO) l'accès à des documents concernant la modification de l'extension de la Convention collective de travail pour la retraite anticipée des travailleurs dans le second œuvre de Suisse romande. Le SECO a refusé l'accès à ces documents en invoquant l'absence de droit d'accès aux documents durant la procédure d'extension de la convention générale de travail, ajoutant qu'il s'agissait dans le cas présent de documents pertinents relatifs à l'arrêt imminent du Conseil fédéral. Dans sa recommandation, le Préposé a approuvé la prise de position du SECO selon laquelle il s'agissait d'un cas d'application d'une décision administrative en suspens jusqu'à ce qu'un arrêté du Conseil fédéral aura été rendu. Raison pour laquelle les documents officiels ne devaient pas encore être rendus accessibles.

Recommandation SRC / Dossier Espion de la RDA (21 septembre 2012)

Le 22 mai 2012, un demandeur a requis du Service de renseignement de la Confédération (SRC) l'accès au dossier d'un espion de la RDA. Le SRC a refusé cet accès, alléguant qu'il était impossible de donner accès à ces documents pour des

motifs touchant à la sécurité intérieure et extérieure du pays ainsi que dans le but de protéger la personne concernée.

Etant donné que tous les documents indiqués par le demandeur ont été établis avant l'entrée en vigueur de la loi sur la transparence et que, de ce fait, ils n'entrent pas dans le champ d'application de la loi sur la transparence, le Préposé a établi dans sa recommandation que le demandeur ne pouvait pas prétendre à la publication des documents en question.

Recommandation IFSN / Rapport de sécurité Centrale nucléaire Mühleberg (2 octobre 2012)

Le demandeur a requis dans ce cas l'accès aux documents officiels concernant la «prise de position quant au réexamen périodique de sécurité de la centrale nucléaire de Mühleberg» auprès de l'Inspection fédérale de la sécurité nucléaire (IFSN). L'IFSN a refusé l'accès à tous les documents en alléguant qu'une partie d'entre eux n'entrent pas dans le champ d'application temporel de la loi sur la transparence. En outre, tous les autres documents font à son avis partie du dossier d'une procédure administrative en cours et, de ce fait, n'entrent pas dans le champ d'application matériel de la loi. Dans sa recommandation, le Préposé a également conclu que parmi les documents désignés par le demandeur, une partie n'entre effectivement pas dans le champ d'application temporel de la loi sur la transparence et qu'une autre partie n'entre pas dans le champ d'application matériel de la même loi. Il a donc soutenu la position de l'IFSN consistant à refuser l'accès à l'ensemble des documents.

Recommandation AFC / Projet INSIEME (5 octobre 2012)

Le demandeur a requis de l'Administration fédérale des contributions (AFC) l'accès à une liste comprenant les noms et les données de toutes les entreprises ayant fourni des prestations pour le projet informatique INSIEME ou avec lesquelles des contrats de prestations ou de livraison avaient été conclus. L'AFC n'a pas accordé l'accès demandé immédiatement, mais l'a repoussé jusqu'à la clôture de la procédure pénale entre-temps engagée. Le Préposé est parvenu au même résultat dans sa recommandation.

Recommandation fedpol / Acquisitions décentralisées (19 octobre 2012)

Le demandeur a requis de l'Office fédéral de la police (fedpol) l'accès à un rapport sur des acquisitions décentralisées. Fedpol en a refusé l'accès notamment au motif que le rapport permettrait de tirer des conclusions sur les procédés de tactiques policières de la Police judiciaire fédérale. Ce qui pourrait entraver les enquêtes judiciaires et mettre en danger ses collaborateurs. Dans sa recommandation, le Préposé a précisé en premier lieu que les documents en question étaient surtout constitués de la correspondance de fedpol avec l'Office fédéral des constructions et de la logistique et avec la Commission des achats de la Confédération. En outre, un tableau était concerné présentant entre autres une liste des objets acquis (par ex. vignettes automobiles, armoires et agrafes), des partenaires contractuels et les frais totaux des acquisitions. Le Préposé a conclu dans sa recommandation que le mandat de protection et l'activité d'enquête de fedpol pouvaient sans problème être poursuivis même si les documents étaient divulgués et que la mise en œuvre conforme aux objectifs fixés par les autorités ainsi que la réussite des enquêtes n'était pas entravée par la communication des objets acquis. En outre, le Préposé estimait que l'intérêt public à un accès illimité aux documents primait sur la protection de la sphère privée des partenaires contractuels et que les collaborateurs de fedpol n'avaient pas à craindre de répercussions négatives d'une divulgation de leurs données personnelles. En conséquence, il a recommandé l'accès aux données personnelles.

Recommandation ChF / Décision du Conseil fédéral concernant la transmission de données d'employés au Département américain de la justice (19 octobre 2012)

La demanderesse a déposé une demande d'accès auprès de la Chancellerie fédérale (ChF) afin d'obtenir une copie de la décision prise par le Conseil fédéral concernant la transmission par certaines banques suisses de données relatives à leurs employés au Département américain de la justice. La ChF a refusé d'accorder l'accès au document requis, d'une part, car il s'agissait d'une décision prise par le Conseil fédéral dans le cadre d'une procédure de co-rapport et d'autre part parce qu'une procédure pénale était en cours. Le Préposé a établi dans ses conclusions que la ChF n'avait pas l'obligation d'accorder l'accès au document requis par la demanderesse car les décisions du Conseil fédéral font partie intégrante de la procédure de co-rapport et ne sont pas soumises à la loi sur la transparence.

Recommandation CDF / Rapport d'audit Immobilier (12 novembre 2012)

La demanderesse a requis l'accès au rapport daté de fin 2010 du Contrôle fédéral des finances (CDF) «Audit de surveillance du Contrôle fédéral des finances armasuisse Immobilier». Le CDF n'a accordé qu'un accès partiel, réclamant en outre une taxe de 400 francs. La demanderesse n'était d'accord ni avec la restriction de l'accès, ni avec les 400 francs de taxes et déposa une demande de médiation auprès du Préposé. Le CDF a par contre fait valoir d'une part qu'il avait accordé un accès total aux documents et d'autre part que la loi sur la transparence ne prévoyait pas la possibilité d'une procédure de médiation en cas de contestation des émoluments. Dans sa recommandation, le Préposé a estimé que les émoluments pouvaient varier en fonction du volume de documents auxquels l'accès était accordé et que de ce fait, il y avait une relation étroite entre la question des faits et la question des coûts. De ce fait, le Préposé a considéré licite sur le principe de contester dans une demande de médiation à la fois la restriction de l'accès et le montant des émoluments demandés. Par ailleurs, le Préposé a établi que la confirmation de la demande conformément à l'article 16 alinéa 2 de l'ordonnance sur la transparence (OTrans) n'était ni une acceptation du montant des émoluments, ni une déclaration de renoncement à un recours ultérieur. Enfin, il a précisé à propos du calcul des émoluments qu'en matière de transparence, le principe d'équivalence n'était applicable qu'avec réserve. Le montant des émoluments ne doit pas entraver le principe qui sous-tend la loi sur la transparence, à savoir permettre l'accès aux documents officiels, et déployer un effet dissuasif. Ainsi, concrètement, compte tenu de l'effet utile du droit d'accès, le prélèvement d'un émolument moins élevé est de mise même si la charge de travail sur le plan administratif justifierait objectivement un montant plus élevé. Par ailleurs, on ne peut guère à partir de la loi sur la transparence établir une équivalence entre la prestation administrative et la contreprestation financière. En conclusion, le Préposé a recommandé l'accès entier au rapport d'examen et le réexamen du montant de l'émolument demandé.

Recommandation Swissmedic / Vérification de la licéité de produits médicaux (4 décembre 2012)

Le demandeur A a requis l'accès à des documents officiels de l'Institut suisse des produits thérapeutiques Swissmedic sur lesquels était effectuée une vérification de légalité de la publicité et la vente de certains produits médicaux. Swissmedic a accordé au demandeur A un accès partiel. A la suite duquel il a requis une médiation. Parmi les très nombreux documents, l'Institut en avait caviardé certains entièrement en raison de la présence de secrets professionnels et de fabrication

(notamment sur environ 20 pages), et certains autres partiellement en raison de la présence de données personnelles. Concernant une petite partie, Swissmedic a repoussé l'accès, car un tiers concerné (le demandeur B) s'opposait à la publication de ses données personnelles. Après la demande en médiation déposée par A, B a également fait une demande auprès du Préposé, en invoquant le fait que les documents en question étaient extraits du dossier d'une procédure administrative et administrative pénale. En outre, il estimait qu'il était impossible d'anonymiser les documents qui le concernaient, car dans sa lettre, la présentation et la typographie spécifique à l'entreprise suffisaient à elles seule à l'identifier comme auteur des documents. Swissmedic a repoussé dans le temps l'accès à ces documents, tout en estimant que les documents concernant B ne faisaient pas partie d'une procédure administrative et administrative pénale. Dans sa recommandation, le Préposé a conclu que Swissmedic avait appliqué correctement la loi sur la transparence et que le demandeur A s'était vu accordé à juste titre et de manière appropriée un accès restreint aux documents demandés. Il a par ailleurs qualifié de raisonnables les émoluments facturés par Swissmedic. A propos de B, il a considéré que sa correspondance professionnelle ne présentait pas de caractéristiques spécifiques, donc qu'il n'était pas aisément possible d'identifier l'auteur du document. En outre, il se rallia à l'estimation de Swissmedic selon laquelle les documents officiels qui concernaient le demandeur B ne faisaient pas partie d'une procédure administrative et administrative pénale. Il a donc recommandé à Swissmedic de remettre également ces documents à A.

Recommandation CDF / Vérification de la licéité d'émoluments, droit de déposer une demande en médiation avant l'appréciation de la demande d'accès (4 décembre 2012)

Le demandeur a requis l'accès au rapport «Conduite de la guerre électronique; vérification de la rentabilité et de l'engagement de systèmes du DDPS, du 30 septembre 2009», établi par le Contrôle fédéral des finances (CDF). Le CDF a estimé que le document officiel en question était un rapport classé confidentiel, raison pour laquelle il fallait encore, entre autres, vérifier avec l'unité administrative concernée si le rapport demandé pouvait être déclassé. Le CDF a en outre informé le demandeur que les émoluments s'élèveraient probablement entre 8000 et 10 000 francs. Sur ce, le demandeur a déposé auprès du Préposé une demande en médiation, en le priant de vérifier si le montant des émoluments que le CDF lui avait communiqué pour pouvoir consulter le rapport en question étaient justifiés. Dans sa recommandation, le Préposé a établi que le demandeur était exceptionnellement habilité à déposer une demande en médiation avant l'examen

matériel de la demande d'accès. Car la quantité de travail était supposément excessive. Il a également fait remarquer que le montant annoncé était si excessif qu'il équivalait en définitive à une limitation ou à un refus de l'accès.

Recommandation OFPER / Liste des primes payées dans l'administration fédérale (6 décembre 2012)

Le demandeur a requis de l'Office fédéral du personnel (OFPER) l'accès à une liste des primes versées dans l'administration fédérale. L'OFPER a opposé un refus à cette demande en invoquant l'argument que les informations demandées ont été établies sur mandat de la Délégation des finances (DélFin) et faisaient de ce fait partie de documents de la délégation et de la commission de la DélFin. Conformément à la loi sur le Parlement, les délibérations et les procès-verbaux des commissions sont confidentiels. Il ressort des documents que la DélFin a fait parvenir au Préposé que la liste demandée avait été établie par l'OFPER, sur mandat écrit exprès de la DélFin. En raison de la norme spéciale de protection du secret que constitue la loi sur le Parlement, la loi sur la transparence n'est pas applicable aux documents mandatés explicitement par la DélFin. De ce fait, de l'avis du Préposé, le demandeur ne pouvait invoquer aucun droit d'accès aux documents en question et il recommanda donc à l'OFPER de maintenir son refus.

Recommandation OFAC / Dossier d'une procédure administrative pénale engagée contre une compagnie d'aviation (18 décembre 2012)

Le demandeur a requis de l'Office fédéral de l'aviation civile (OFAC) l'accès à des documents officiels concernant une procédure administrative pénale engagée contre une compagnie aérienne. Plus concrètement, il désirait consulter tous les documents qui concernaient la communication d'un passager à propos d'un vol retardé, ainsi que tous les documents y relatifs qui résultaient de l'appréciation de cet état de fait par l'OFAC et de sa décision de ne pas sanctionner la compagnie d'aviation dans ce cas. L'office refusa au demandeur l'accès aux documents en invoquant le fait que les documents extraits de dossiers d'une procédure (administrative) pénale ne relevaient pas du champ d'application de la loi sur la transparence. Dans le cadre de la procédure en médiation, le Préposé a mis à plusieurs reprises l'OFAC en demeure de lui remettre les documents en question afin d'examiner s'il était éventuellement possible d'en autoriser la consultation. L'Office maintenait à ce propos que le Préposé n'avait pas besoin de consulter les documents en question pour examiner la question de principe à laquelle il fallait répondre en l'occurrence, à savoir, si la loi sur la transparence donnait à des tiers un droit d'accès au dossier d'une procédure administrative pénale. Contrairement aux commentaires figurant dans le message du Conseil fédéral

relatif à la loi sur la transparence, le Préposé a établi dans sa recommandation, en se fondant sur la doctrine, que les documents officiels d'une procédure déjà close relevaient néanmoins du champ d'application de la loi sur la transparence. Cela n'était toutefois valable qu'à la condition que les documents aient déjà existé avant l'ouverture de la procédure et n'aient pas été explicitement établis pour la procédure. Du fait que l'OFAC refusait de remettre les documents au Préposé, celui-ci n'avait aucune possibilité de juger si au moins une partie des documents en question dataient d'avant l'ouverture de la procédure. Par conséquent, et conformément au principe «dans le doute, pour la transparence», il a, dans sa recommandation, enjoint l'OFAC d'accorder l'accès à tous les documents énoncés par le demandeur.

2.3.2 Médiations

Une solution consensuelle a été trouvée dans les cas suivants:

Médiation DFAE / Rapport d'inspection et convention de départ

Le demandeur a requis du DFAE l'accès à un rapport d'inspection interne datant de 2005 ainsi que la convention de départ concernant la dissolution d'un rapport de service entre le département et une personne employée. Le DFAE et le demandeur se sont accordés sur la communication d'une information extraite de la convention de départ, ce qui nécessitait toutefois encore l'accord du tiers concerné. Ce dernier étant consentant, un accord a pu être trouvé. Le demandeur a en outre reconnu que le rapport d'inspection avait été établi avant l'entrée en vigueur de la loi sur la transparence et que de ce fait, il ne pouvait invoquer pour lui-même un droit d'accès.

Médiation Fonds national suisse / Esquisses de projets

La demanderesse a requis l'accès aux travaux de recherche qui avait été remis au Fonds National Suisse (FNS) dans le cadre des Programmes nationaux de recherche (PNR 57). Elle voulait l'accès à tous les documents du projet de recherche avant que les résultats des chercheurs ne soient officiellement publiés. Elle désirait en outre la traduction des résumés des études ainsi que des éventuels commentaires récapitulatifs en allemand, français et italien. Ultérieurement, elle déposa encore une demande d'accès. Au cours des pourparlers de médiation, les parties sont parvenues à un accord à propos des deux demandes: il allait être demandé à onze groupes de chercheurs si le FNS pouvait publier leurs rapports finaux.

2.4 Décisions judiciaires relatives à la loi sur la transparence

2.4.1 Tribunal administratif fédéral

Au cours de l'exercice 2012, le Tribunal administratif fédéral (TAF) a rendu trois arrêts en relation avec l'accès à des documents officiels; deux d'entre eux faisaient suite à une procédure de médiation auprès du Préposé.

L'Office fédéral des assurances sociales (OFAS) a rendu une décision contre la recommandation du Préposé du 22 décembre 2012 (cf. notre 19e rapport d'activités 2011/2012, ch. 2.3.1). Par la suite, un recours a été formé contre la décision de l'OFAS auprès du TAF. Le service de comptabilité mandaté au niveau interne par le recourant a laissé passer le délai établi par le Tribunal pour fournir une avance de frais. Le Tribunal a rejeté la demande de restitution du délai au motif que des insuffisances en matière d'organisation ne pouvaient pas être considérées comme un motif d'empêchement non fautif. Le Tribunal a laissé ouverte la question de savoir si le recourant pouvait retenter la procédure d'accès en déposant une nouvelle demande, et obtenir par ce moyen une nouvelle décision, ou si la force de chose jugée de la décision d'instance préalable s'opposait à cette procédure (arrêt du 12 avril 2012, réf. A-884/2012).

Après la recommandation du 6 juillet 2011 (cf. notre 19e rapport d'activités 2011/2012, ch. 2.3.1), le Secrétariat d'Etat à l'économie SECO a demandé au Préposé de modifier cette recommandation car entre-temps, une procédure pénale était en suspens en la cause. Le Préposé ne pouvait pas donner suite à cette demande, ne serait-ce que pour des raisons formelles car la loi sur la transparence ne prévoit pas ce genre de possibilité. Le SECO a ensuite rendu une décision par laquelle il suspendait sa décision sur le fond concernant l'accès aux documents demandés jusqu'à la clôture définitive de la procédure pénale citée. Le recourant a déposé contre cette décision un recours pour retard injustifié auprès du TAF. Celui-ci a examiné en détail les différentes phases de la procédure de demande d'accès et a approuvé le retard injustifié. Par voie de conséquence, l'affaire a été renvoyée au SECO pour réexamen matériel (arrêt du 15 mai 2012, réf. A-6037/2011).

Dans un autre cas, le TAF s'est penché sur la question de savoir si l'obligation de s'acquitter d'un émolument prévue par la loi sur la transparence était également valable pour les professionnels des médias. Un journaliste avait demandé l'accès à des informations concernant le contrôle des étiquettes-énergie des appareils électriques par Electrosuisse et par l'Inspectorat fédéral des installations à courant fort (ESTI). Après examen des documents, l'Office fédéral de l'énergie (OFEN) a

informé le demandeur du montant probable de 200 francs des émoluments, suite à cela le demandeur a informé l'OFEN qu'il maintenait sa demande. Après avoir été informé du montant des émoluments entre-temps passés à 250 francs et obtenu un accès partiel aux documents suite au caviardage de certains passages, le demandeur a requis de l'OFEN une décision sur les émoluments et une indication des voies de droit. Le journaliste a attaqué cette décision en invoquant le fait qu'elle allait à l'encontre de la volonté du législateur car le prélèvement des émoluments ne tenait pas compte des besoins spécifiques et du rôle spécial des médias et, de ce fait, minait le principe de la transparence. Dans son arrêt, le TAF a par contre exprimé l'avis selon lequel le Conseil fédéral, dans son message relatif à la loi sur la transparence, avait certes pris en considération des facilités quant au prélèvement des émoluments pour les professionnels des médias, mais n'avait prévu dans l'ordonnance sur la transparence (OTrans) aucune libération générale des médias de l'obligation générale de s'acquitter des émoluments. De son point de vue, une libération des émoluments pour les journalistes serait difficilement conciliable avec le principe d'égalité devant la loi. Par contre, l'ordonnance générale sur les émoluments (OGEmol) prévoit que les émoluments ne sont pas prélevés quant la décision ou la prestation sert un intérêt prépondérant. Ainsi, selon le TAF, il faudrait, dans le domaine de la loi sur la transparence, mettre en balance l'intérêt public à un accès aux documents et l'intérêt à une administration rationnelle et efficace. Pour cette raison, il pourrait y avoir abandon de l'obligation de s'acquitter des émoluments s'il s'agissait de prestations de nature existentielle pour l'Etat ou pour l'individu – donc pour le public. Le TAF précisa encore que l'on ne pouvait pas mettre sur un pied d'égalité l'intérêt public prépondérant d'une manière générale avec les projets des journalistes qui, selon les cas, intéressent une partie plus ou moins grande de la population.

En définitive, le TAF a déclaré de manière explicite qu'un émolument peut aussi être prélevé auprès des journalistes qui désirent accéder à des documents officiels. A propos du prélèvement concret des émoluments il mentionnait que chaque document devait être contrôlé, phrase pour phrase, et non pas seulement les désignations et les noms de tiers, ce qui pouvait se traduire par une charge de travail non négligeable. Le Tribunal a considéré les 250 francs imposés par l'instance inférieure comme appropriés et a rejeté le recours (arrêt du 27 novembre 2012, réf. A-1200/2012)

2.5 Consultation des offices et autres prises de position

2.5.1 Entrée en vigueur du nouveau droit comptable

Le Préposé s'est prononcé dans le cadre d'une consultation des offices concernant l'ouverture de l'audition relative à l'entrée en vigueur du droit comptable et aux dispositions d'exécution (ONCR et révision partielle OSRev). Le projet prévoyait entre autres une exception de l'autorité fédérale de surveillance en matière de révision (ASR) du champ d'application personnel de la loi sur la transparence. Le Préposé a certes reconnu d'une part que l'activité de surveillance de l'ASR nécessitait selon les cas une protection qualifiée. D'autre part, il a souligné que la loi sur la transparence offrait en l'espèce suffisamment de moyens légaux pour protéger les secrets professionnels et les secrets de fabrication ainsi que les données personnelles. L'ASR s'est rallié à cette position au terme d'une réunion à laquelle étaient représentés le Préposé et l'Office fédéral de la justice.

2.5.2 Interpellation urgente: Halte à l'extension rampante du champ d'application des conventions collectives aux entreprises d'autres branches

Dans le cadre d'une consultation des offices, le Préposé s'est prononcé sur le projet de réponse du Conseil fédéral à une interpellation urgente concernant l'application de la loi sur la transparence aux procédures d'extension des conventions collectives. Le projet de réponse mentionnait à juste titre que durant la procédure d'extension, la loi sur la transparence ne permettait pas de déduire un droit d'accès, car la décision politique et administrative n'avait pas encore été prise en l'espèce. Le Préposé a proposé un complément selon lequel une fois rendue la décision concernant la procédure d'extension, les exceptions de la loi sur la transparence sont applicables à titre subsidiaire.

2.5.3 Définition des nouveaux tarifs des analyses de laboratoire: transparence renforcée dans la procédure

La Commission de gestion du Conseil national (CdG-N) a établi sept recommandations dans le cadre de son enquête sur la légalité et la conformité de la procédure concernant la définition des nouveaux tarifs des analyses de laboratoire à la loi fédérale sur l'assurance-maladie (LAMal). Après avoir demandé une première fois au Conseil fédéral de se prononcer, la CdG-N lui a à nouveau demandé de prendre position. La CdG-N a requis dans l'une de ses recommandations que le Conseil

fédéral examine dans quelle mesure les personnes concernées peuvent avoir un meilleur accès aux résultats intermédiaires de la procédure. Notamment, au contenu des prises de position de l'OFSP et des experts externes, ainsi qu'aux recommandations de la Commission fédérale des analyses, moyens et appareils à l'intention du DFI. Dans ce contexte, le Conseil fédéral devait identifier les obstacles juridiques qui s'opposent éventuellement à une plus grande transparence de la procédure et esquisser des solutions.

Le Préposé a recommandé que dans la réponse du Conseil fédéral, une distinction claire soit faite entre le mode actif et le mode passif du processus d'information et qu'il soit mentionné explicitement qu'une autorité peut communiquer une information de manière active même si on ne peut en déduire un droit d'accès conformément à la loi sur la transparence. L'OFSP a tenu compte de nos commentaires et a procédé aux modifications nécessaires.

2.5.4 Projet de loi sur le renseignement

Dans le cadre de la consultation des offices, le Préposé s'est prononcé sur le projet de loi sur le renseignement (LRens). Ce projet prévoit l'exclusion du champ d'application personnel de la loi sur la transparence des cas relatifs au Service de renseignement de la Confédération (SRC). Le Préposé a rejeté le projet en se référant notamment à la logique de la loi sur la transparence qui repose sur trois piliers:

- Suivant le premier pilier, toutes les autorités de la Confédération tombent, en principe, sous le champ d'application personnel de la loi sur la transparence.
- Suivant le deuxième pilier, tous les documents officiels tombent en principe dans le champ d'application de la loi sur la transparence.
- Suivant le troisième pilier, la loi sur la transparence prévoit un système selon lequel l'accès à des documents officiels émanant des autorités repose, dans des cas spécifiques, sur une pesée des intérêts.

Afin de tenir compte du fait que certaines informations officielles nécessitent une protection particulière, les articles 7 à 9 LTrans en particulier renferment une longue liste de possibilités légales de limiter, différer ou refuser l'accès à un document officiel. De l'avis du Préposé, il est ainsi tout à fait possible, justement dans le cas de documents du SRC, de tenir compte des circonstances concrètes lorsqu'il s'agit d'informations particulièrement sensibles. Le Préposé a ainsi contredit de manière décisive l'argumentation du SRC selon laquelle son besoin spécifique de

protection n'était pas compatible pour des raisons de principe avec la notion de transparence concrétisée dans la loi.

Par ailleurs, au vu des statistiques annuelles communiquées jusqu'ici par le DDPS, le Préposé a exprimé son désaccord à propos de l'argument du SRC selon lequel les demandes d'accès conformément à la loi sur la transparence se traduisaient, pour le DDPS, par un surplus de travail considérable. Enfin, le Préposé a relevé que les récents événements survenus au sein de l'administration (en particulier dans le contexte du projet «Insieme» de l'Administration fédérale des contributions et du vol de données au SRC au cours de l'exercice écoulé) ont une fois de plus montré l'importance de la transparence dans le cadre de la mission, l'organisation et l'activité de l'administration.

Attendu que le DDPS n'a pas tenu compte des propositions formulées par le Préposé, ce dernier a rédigé un co-rapport à l'attention du Conseil fédéral. Contrairement à ce qu'il avait proposé dans le cadre de la procédure de consultation, le DDPS a - selon les termes du nouveau projet – dès lors proposé d'exclure totalement du champ d'application matériel de la loi sur la transparence la «recherche d'information par le SRC». Le Préposé a contesté la comparaison opérée par le DDPS, selon laquelle «la recherche d'informations par le SRC» serait comparable à une procédure judiciaire et ne devrait par conséquent pas être soumise à la loi sur la transparence. A ce sujet, il convient également de relever que les lois de procédure prévoient précisément un droit de consulter le dossier pour les parties et n'excluent pas par principe la consultation. Le Préposé a aussi critiqué la formulation très générale du terme «recherche d'information par le SRC», moyennant laquelle la tâche principale du Service de renseignement – et ainsi en définitive la totalité de celle-ci – serait complètement exclue du champ d'application de la loi sur la transparence.

Le Conseil fédéral n'a pas fait siennes les réserves émises par le Préposé. Ceci est d'autant plus regrettable compte tenu du sens et de l'objectif poursuivis par la loi sur la transparence, dans la mesure où la population se voit ainsi privée de tout droit à la transparence, à tout le moins s'agissant des activités des services de renseignement, exercées de façon non reconnaissable et par voie de conséquence dans des domaines inconnus.

Voir à ce sujet le ch. 1.4.6 du présent rapport d'activités.

2.6 Divers

2.6.1 Journée sur la transparence

Le 24 février 2012, en collaboration avec l'Office fédéral de la justice, le Préposé a organisé la «Journée de la transparence», à l'intention des conseillers à la transparence de l'administration fédérale. Cette rencontre avait pour but d'une part un échange d'expériences, entre les autorités chargées de l'application des lois, à propos de la mise en œuvre pratique du principe de la transparence, et d'autre part de fournir des réponses aux questions concrètes souvent posées.

Sur la base des résultats de cette rencontre, le Préposé et l'Office fédéral de la justice ont remanié et actualisé le document «Mise en œuvre du principe de la transparence dans l'administration fédérale: questions fréquemment posées», datant de l'année 2010. Ce document peut être consulté sur notre site www.leprepose.ch Principe de la transparence – FAQ sur la mise en œuvre du principe de transparence.

2.6.2 Relations avec les services de conciliation – Groupe de travail sur la Médiation

Le PFPDT n'est pas la seule autorité en Suisse qui mène des procédures de conciliation ou de médiation dans le domaine du principe de la transparence. Plusieurs cantons connaissent cette procédure informelle permettant la résolution des différends en relation avec la consultation de documents officiels. La collaboration et l'échange d'expériences étant importants pour le PFPDT et pour les préposés cantonaux à la transparence, le Groupe d'intervision sur la gestion consensuelle des conflits transparence a été fondé en automne 2011. Durant l'exercice écoulé, des rencontres régulières ont permis aux autorités participantes un intense échange d'expériences sur des questions touchant au principe de la transparence et à la médiation.

3. Le PFPDT

3.1 La septième Journée de la protection des données

Dans le contexte de la septième Journée de la protection des données, le PFPDT a publié le 28 janvier 2013 une brochure portant sur la protection des données et de la personnalité au travail. Conjointement, une nouvelle version du service en ligne «ThinkData» a été présentée lors d'une conférence qui s'est tenue près de Lausanne. Ce service est à la disposition des autorités et des entreprises pour répondre aux questions touchant à la protection des données et à la transparence.

La sphère privée est un bien fondamental qui requiert une protection particulière. Ceci vaut également dans le monde du travail, c'est aspect auquel l'employeur doit porter une attention particulière. Cependant, comme l'explique la petite brochure «Protection des données et de la personnalité sur le lieu de travail: un droit légitime», la sphère privée de l'employé s'arrête là où commencent les intérêts commerciaux de l'employeur ou là où elle entre en conflit avec la loi. Conçue comme une introduction à la problématique, cette brochure informe sur les obligations de l'employeur lorsqu'il installe une vidéosurveillance, sur les dispositions à prendre lorsqu'un employé passe trop de temps à surfer sur la toile ou sur le fait que l'employeur ne peut consulter que des sources accessibles au public lorsqu'il veut s'informer sur des postulants. La brochure peut être commandée gratuitement auprès du Préposé et téléchargée à partir du site www.le.prepose.ch.

Le traitement des données dans les entreprises est également une préoccupation centrale du service en ligne ThinkData, dont la nouvelle version a été présentée au public dans le cadre d'une conférence qui s'est tenue à Chavannes-près-Renens. Le site www.thinkdata.ch offre aux entreprises, aux autorités et aux organisations des informations et des conseils adaptés à leurs besoins pour qu'elles puissent assurer un traitement approprié des données personnelles (cf. notre 19e rapport d'activités 2011/2012, ch. 3.2). Le site ThinkData est géré par un groupe de travail interdisciplinaire dont le PFPDT a pris la direction début 2013.

Par ailleurs, le professeur Ebrahimi Touradj, de l'EPFL, a tenu lors de cette conférence un exposé sur les avantages et les risques liés à la vidéosurveillance en illustrant notamment la manière dont ce type de technologie peut être utilisé, en conformité avec les règles applicables à la protection des données. Le débat auquel ont participé Alexis Roussel, vice-président du Parti Pirate Suisse, Jean-Philippe Walter, préposé suppléant du PFPDT, et d'autres experts, a porté notamment sur les perspectives de la protection des données à l'heure du tout numérique.

3.2 Publications du PFPDT au cours de l'exercice écoulé

Notre principal canal de publications est le site internet www.leprepose.ch sur lequel les usagers trouvent des informations utiles et des réponses à leurs questions concernant la protection des données et le principe de la transparence. Au cours de l'exercice écoulé, la large palette de thèmes présentés a été enrichie par des commentaires relatifs à la protection des données lors des manifestations sportives populaire, dans les bibliothèques ainsi qu'à propos de la mise au pilori sur internet. En outre, nous avons publié une brochure sur la protection des données et de la personnalité dans le domaine du travail.

La mise au pilori sur internet est une pratique qui rencontre une popularité croissante. Elle consiste à publier des listes noires qui contiennent les noms de personnes dont le comportement ou les décisions n'ont pas convenu à l'auteur de la liste. Souvent, elles indiquent même l'adresse privée et la photographie des personnes en question, ce qui soulève un certain nombre de questions juridiques du point de vue de la protection des données (cf. ch.1.3.1 du présent rapport d'activités). Vous trouverez des informations plus détaillées à ce propos sur notre site internet www.leprepose.ch à la rubrique Protection des données – Internet et ordinateur.

Des milliers de sportifs amateurs participent chaque année à de nombreuses manifestations de sport populaire comme le gigathlon ou autres marches populaires. Des données personnelles sont également traitées à cette occasion et souvent, il arrive que ces traitements aillent plus loin que ne l'exige le déroulement de la rencontre. Ces pratiques ne sont pas sans poser quelques problèmes du point de vue de la protection des données (cf. ch. 1.2.5 du présent rapport d'activités). Nos commentaires à ce propos se trouvent sur notre site, à la rubrique Protection des données – Loisirs et sport.

Au cours de l'exercice écoulé, nous avons également publié des commentaires sur la protection des données dans les bibliothèques. Les bibliothèques sont obligées de traiter des données personnelles pour gérer administrativement le prêt des livres. D'autres prestations, comme la mise à disposition de postes de travail connectés à internet, touchent également aux données personnelles. Celles-ci sont moins anodines qu'elles n'en ont l'air au premier coup d'œil. Une fois agrégées entre elles, elles peuvent permettre d'établir des profils de la personnalité très instructifs (Protection des données – Statistique, registre et recherche).

Cette année, nous avons également associé nos efforts à ceux de l'Office fédéral de la justice pour développer les Questions fréquemment posées dans la mise en œuvre du principe de transparence au sein de l'administration fédérale. Ce document sert de guide aux autorités fédérales qui traitent les demandes d'accès et peut être consulté sur notre site, aux rubriques Principe de la transparence – Documentation / outil de travail – FAQ pour l'administration fédérale.

Les informations concernant l'utilisation des outils d'analyse pour les sites internet dans l'administration fédérale s'adressent aux mêmes destinataires. Ces outils permettent aux exploitants de sites web d'évaluer les accès des utilisateurs, entre autres pour optimiser leur offre en ligne. Nous avons donc établi un document qui expose les conditions à respecter du point de vue de la protection des données à l'intention des organes fédéraux (à consulter sur notre site internet, aux rubriques Protection des données – Internet et ordinateur).

Enfin, nous avons publié à l'occasion de la septième Journée de la protection des données une brochure portant sur la protection des données et de la personnalité sur le lieu de travail. Elle s'adresse autant aux autorités qu'aux entreprises pour leur rappeler leurs droits et leurs devoirs. La vidéosurveillance sur le lieu de travail est l'un des thèmes traités dans cette petite brochure illustrée, ainsi que l'utilisation d'internet à des fins privées et la recherche en ligne dans le cadre de postulations d'emploi. Pour plus de détails, voir sur notre site, aux rubriques Protection des données – Secteur du travail.

3.3 Participation au Conseil informatique et au Comité pour la sécurité informatique de la Confédération

Depuis le début 2012, nous participons au Conseil informatique de la Confédération. C'est l'occasion d'être informés sur les projets de directives et de donner le cas échéant notre avis concernant les aspects de protection des données ou de transparence impliqués. Nous participons également au Comité pour la sécurité informatique, étant donné les synergies évidentes entre sécurité de l'information et mesures techniques de protection des données.

Depuis l'entrée en vigueur au 01.01.2012 de la révision de l'ordonnance sur l'informatique dans l'administration fédérale (OIAF), le Conseil informatique de la Confédération (CI) est l'organe consultatif de l'Unité de pilotage informatique de la Confédération (UPIC) pour les affaires relatives aux technologies de l'information et de la communication (TIC) nécessitant l'accord des départements et de la Chancellerie fédérale, notamment pour l'édiction de directives et l'approbation de dérogations à leur application. Il se compose du délégué au pilotage informatique de la Confédération et d'un représentant nommément désigné de chaque département et de la Chancellerie fédérale. Un représentant de l'Administration fédérale des finances, du Préposé fédéral à la protection des données et à la transparence (PFPDT), des fournisseurs de prestations internes et des Services du Parlement peut y participer avec voix consultative. Après une année, nous tirons un bilan positif de notre participation régulière au CI et ce à deux titres principaux: être directement informés sur les projets de directives informatiques (notamment en matière de bureautique, de téléphonie, de gestion des affaires et de standardisation de ces produits) et pouvoir, le cas échéant, donner notre avis quant aux aspects de protection des données ou de transparence concernés.

Le Comité de la sécurité informatique (C-SI) est l'organe consultatif de l'UPIC pour toutes les questions de sécurité relatives aux TIC. Il comprend les délégués à la sécurité informatique des départements et de la Chancellerie fédérale. Un représentant du Contrôle fédéral des finances, du PFPDT et des Services du Parlement peut y participer avec voix consultative. Nous y participons depuis plusieurs années, car il y a une synergie évidente entre les problèmes de sécurité de l'information et les mesures techniques de protection des données. Citons par exemple les possibilités offertes par le chiffrement ou la pseudo-anonymisation des données personnelles. Rappelons par ailleurs que la certification organisationnelle en matière de protection des données est essentiellement basée sur la norme ISO/CEI 27001:2005 pour la certification des systèmes de gestion de sécurité de

l'information. Une collaboration a même été institutionnalisée dans le cadre de la formation des responsables de la sécurité informatique des départements ou de leurs offices, afin d'assurer une sensibilisation aux problèmes de protection des données.

3.4 Sensibilisation et formation auprès des étudiants

A la demande de la Faculté de droit de l'Université de Lausanne nous avons présenté, en novembre 2012, notre activité à leurs étudiants en voie master. La présentation prenait place dans le cadre d'un cours interdisciplinaire de la Faculté de droit et des sciences criminelles. Cette intervention portait sur l'activité du Préposé fédéral à la protection des données et à la transparence et présentait, sous la forme d'exemples concrets, des cas de protection des données traités par notre Autorité.

Cette présentation s'est scindée en deux parties. La première avait trait à l'organisation de notre Autorité et les deux axes principaux de notre activité: le conseil et la surveillance. Le mécanisme de contrôle mis en place par notre Autorité a été explicité aux étudiants en recourant à des exemples concrets afin d'en faciliter la compréhension. La présentation s'est poursuivie avec deux cas pratiques qui ont ou continuent de nous occuper. Nous avons ainsi repris l'exemple du cas de jurisprudence en matière de droit d'auteur sous l'angle des développements juridiques de protection des données retenus dans les arrêts du TAF et du TF. Puis nous avons exposé le droit d'accès aux systèmes d'information fédéraux. Enfin, nous avons abordé brièvement les éventuelles modifications de la législation suisse en matière de protection des données induites par la modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Notre intervention auprès d'étudiants s'inscrit dans une démarche générale de sensibilisation et d'information sur les aspects de protection des données que nous déployons dans le cadre de nos activités de conseil et de formation et que nous allons continuer à effectuer dans le futur. Nous constatons une nouvelle fois l'intérêt des étudiants pour a protection des données.

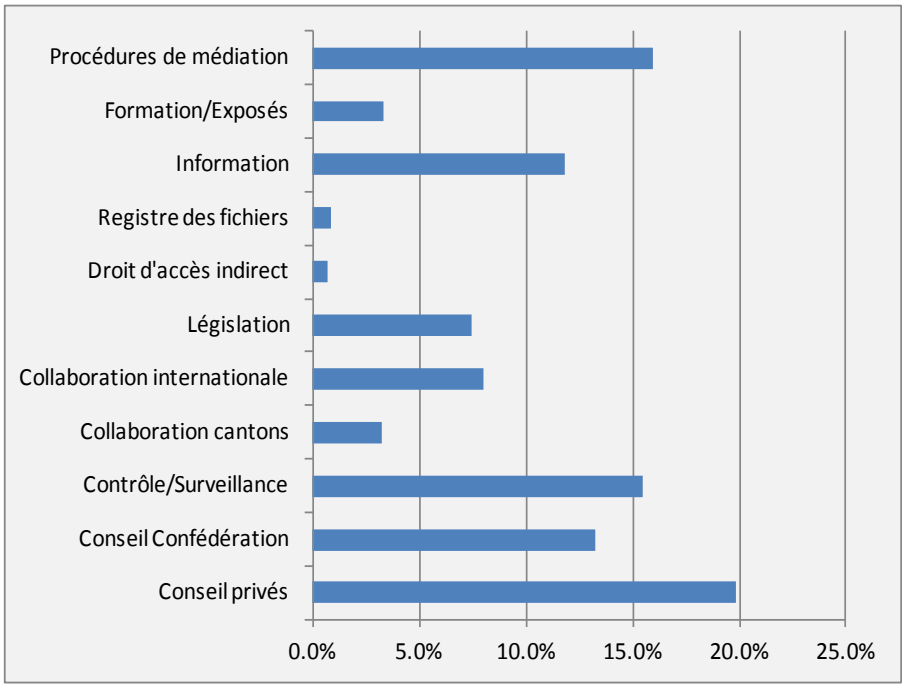
3.5 Formation pour les conseillers en matière de protection des données dans l'administration fédérale

Notre présentation concernant la surveillance sur le lieu de travail lors de deux séances de formation à l'Office fédéral du personnel a suscité beaucoup d'intérêt.

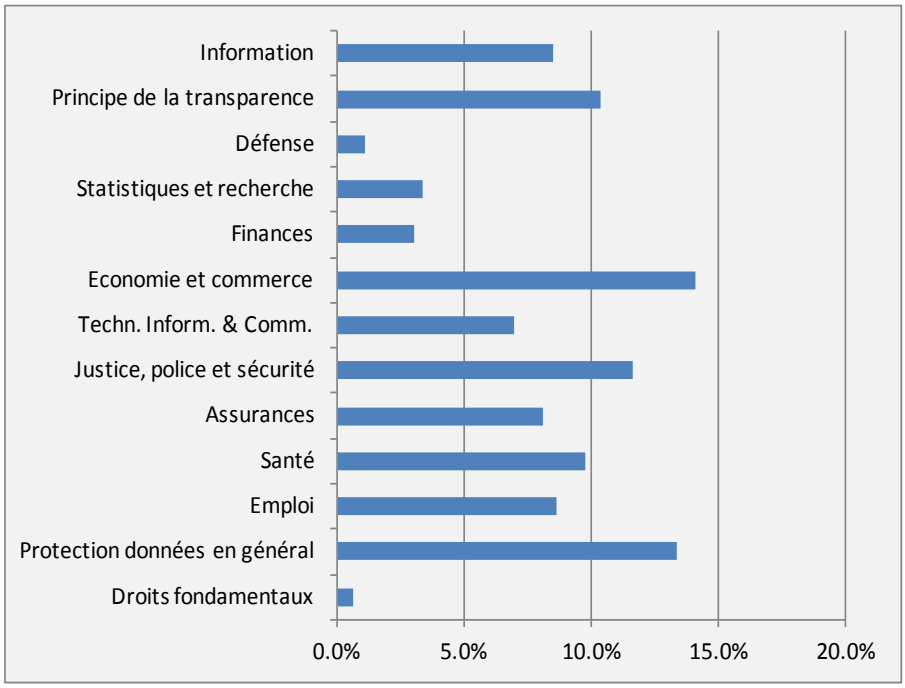
L'année dernière, l'Office fédéral du personnel a mis sur pied une formation continue dans le domaine de la protection des données. Celle-ci s'adresse aux conseillers en matière de protection des données de l'administration fédérale. Nous avons participé aux deux premières séances de formation et y avons fait une présentation sur le thème Surveillance sur le lieu de travail. Nous avons expliqué aux participants les nouvelles dispositions légales pour l'enregistrement et le dépouillement des données des employés de l'administration fédérale et leur avons montré des exemples. Le sujet a suscité un grand intérêt et de nombreuses questions ont été posées. La discussion avec les participants a été utile, car elle a permis d'analyser divers problèmes existants dans le domaine du droit du personnel dans l'administration fédérale. La participation à ces séances nous montre aussi qu'il est judicieux et nécessaire de former les gens à la protection des données.

3.6 Statistique des activités du PFPDT du 1er avril 2012 au 31 mars 2013

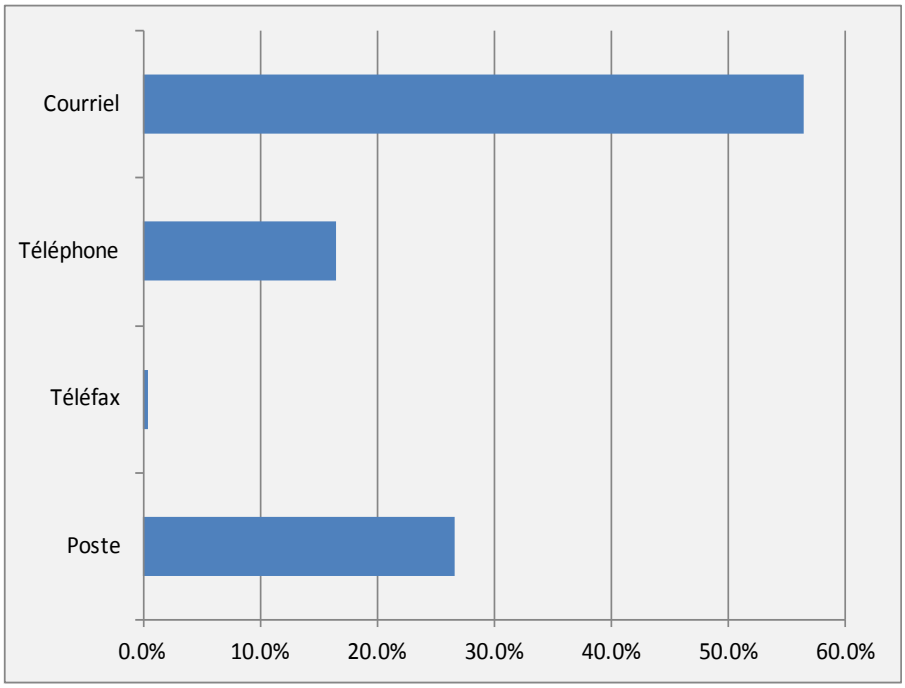
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.7 Statistique des demandes d´accès présentées auprès des départements en vertu de l´art. 6 de la loi sur la transparence (Période: 1er janvier 2012 au 31 décembre 2012)

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
ChF	13	2	5	5	0	1
DFAE	88	57	14	17	0	0
DFI	75	28	23	18	3	3
DFJP	57	28	15	10	1	3
DDPS	34	7	20	7	0	0
DFF	59	19	28	11	0	1
DFE*	80	22	17	31	2	8
DETEC	100	60	16	21	0	3
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 %)	-	-

* depuis le 1er janvier 2013 Département fédéral de l'économie, de la formation et de la recherche DEFR

Chancellerie fédérale ChF

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
ChF	13	2	5	5	0	1
PFPDT	8	6	1	1	0	0
Total	**21**	**8**	**6**	**6**	**0**	**1**

Département fédéral des affaires étrangères DFAE

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
DFAE	88	57	14	17	0	0
Total	**88**	**57**	**14**	**17**	**0**	**0**

Département fédéral de l'intérieur DFI

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	9	4	1	4	0	0
BFEG	0	0	0	0	0	0
OFC	3	1	1	1	0	0
AFS	3	3	0	0	0	0
Météo Suisse	0	0	0	0	0	0
BN	0	0	0	0	0	0
OFSP	24	10	6	6	2	0
OFS	2	1	1	0	0	0
OFAS	11	5	5	1	0	0
SER	1	1	0	0	0	0
Conseil des EPF	2	1	0	1	0	0
MNS	0	0	0	0	0	0
Swiss medic	17	1	7	5	1	3
FNS	0	0	0	0	0	0
SUVA	3	1	2	0	0	0
Total	**75**	**28**	**23**	**18**	**3**	**3**

Département fédéral de justice et police DFJP

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	7	4	1	1	0	1
OFJ	2	1	1	0	0	0
FEDPOL	7	3	2	1	1	0
METAS	5	4	0	1	0	0
ODM	23	11	7	5	0	0
ISDC	2	1	0	1	0	0
IPI	6	4	2	0	0	0
CFMJ	5	0	2	1	0	2
CAF	0	0	0	0	0	0
ASR	0	0	0	0	0	0
CSI	0	0	0	0	0	0
CNPT	0	0	0	0	0	0
Total	**57**	**28**	**15**	**10**	**1**	**3**

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

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	13	3	6	4	0	0
Défense/ armée	8	3	4	1	0	0
SRC	4	0	4	0	0	0
arma-suisse	6	0	4	2	0	0
OFPP	0	0	0	0	0	0
OFSPO	3	1	2	0	0	0
Total	**34**	**7**	**20**	**7**	**0**	**0**

Département fédéral des finances DFF

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	7	5	2	0	0	0
EFV	2	1	0	1	0	0
EPA	3	2	1	0	0	0
ESTV	15	5	5	5	0	0
EZV	8	1	6	1	0	0
EAV	2	1	1	0	0	0
BBL	6	4	0	2	0	0
BIT	3	0	3	0	0	0
EFK	12	0	9	2	0	1
SIF	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
ZAS	0	0	0	0	0	0
Total	**59**	**19**	**28**	**11**	**0**	**1**

Département fédéral de l'économie DFE*

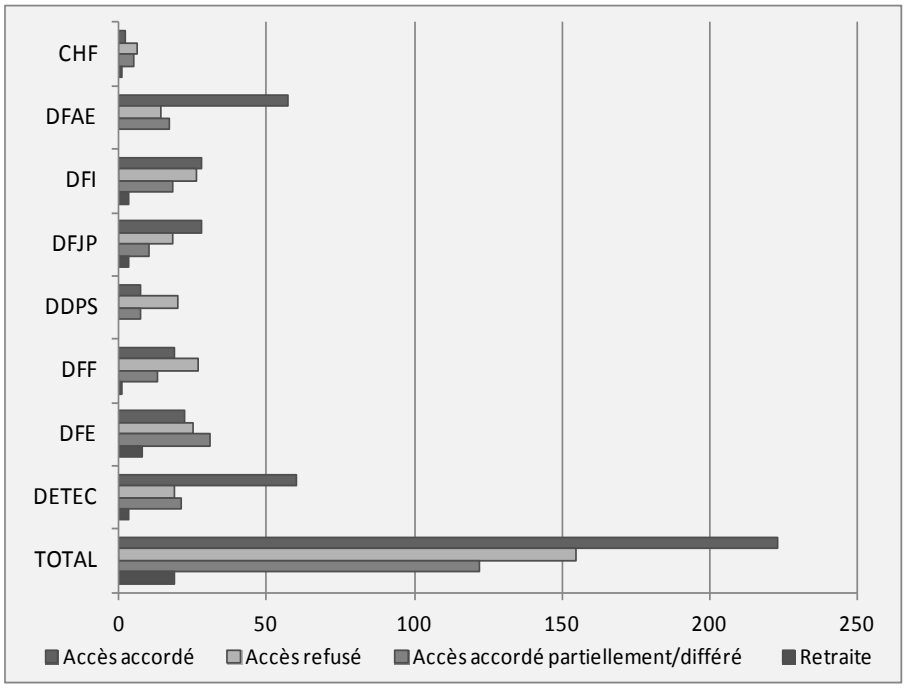
Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	3	0	1	0	1	1
SECO	19	5	7	4	1	2
OFFT	2	1	1	0	0	0
OFAG	21	4	4	8	0	5
OVF	3	2	1	0	0	0
OFAE	0	0	0	0	0	0
OFL	0	0	0	0	0	0
SPr	1	1	0	0	0	0
COMCO	27	9	2	16	0	0
ZIVI	3	0	0	3	0	0
BFC	0	0	0	0	0	0
CTI	1	0	1	0	0	0
IFFP	0	0	0	0	0	0
Total	**80**	**22**	**17**	**31**	**2**	**8**

* depuis le 1er janvier 2013 Département fédéral de l'économie, de la formation et de la recherche DEFR

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

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SG	3	1	1	1	0	0
OFT	10	6	1	3	0	0
OFAC	6	0	5	1	0	0
OFEN	8	2	3	3	0	0
OFROU	4	4	0	0	0	0
OFCOM	11	9	2	0	0	0
OFEV	25	19	2	4	0	0
ARE	2	0	0	2	0	0
ComCom	1	1	0	0	0	0
IFSN	18	6	2	7	0	3
PostCom	0	0	0	0	0	0
AIEP	12	12	0	0	0	0
Total	**100**	**60**	**16**	**21**	**0**	**3**

Traitement des demandes d'accès



3.8 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 2012 au 31 décembre 2012)

Ministère public de la Confédération MPC

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
MPC	4	1	1	2	0	0
Total	**4**	**1**	**1**	**2**	**0**	**0**

3.9 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 2012 au 31 décembre 2012)

Services du Parlement SP

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiel-lement/ différé	Demande d'accès pendante	Retraite
SP	0	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**	**0**

3.10 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2012 au 31 décembre 2012)

Catégorie de requérants	2012
Médias	33
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	21
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	12
Avocats	8
Entreprises	3
Universités	1
Total	**78**

3.11 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:	12 personnes
Unité 3:	5 personnes
Chancellerie:	2 personnes