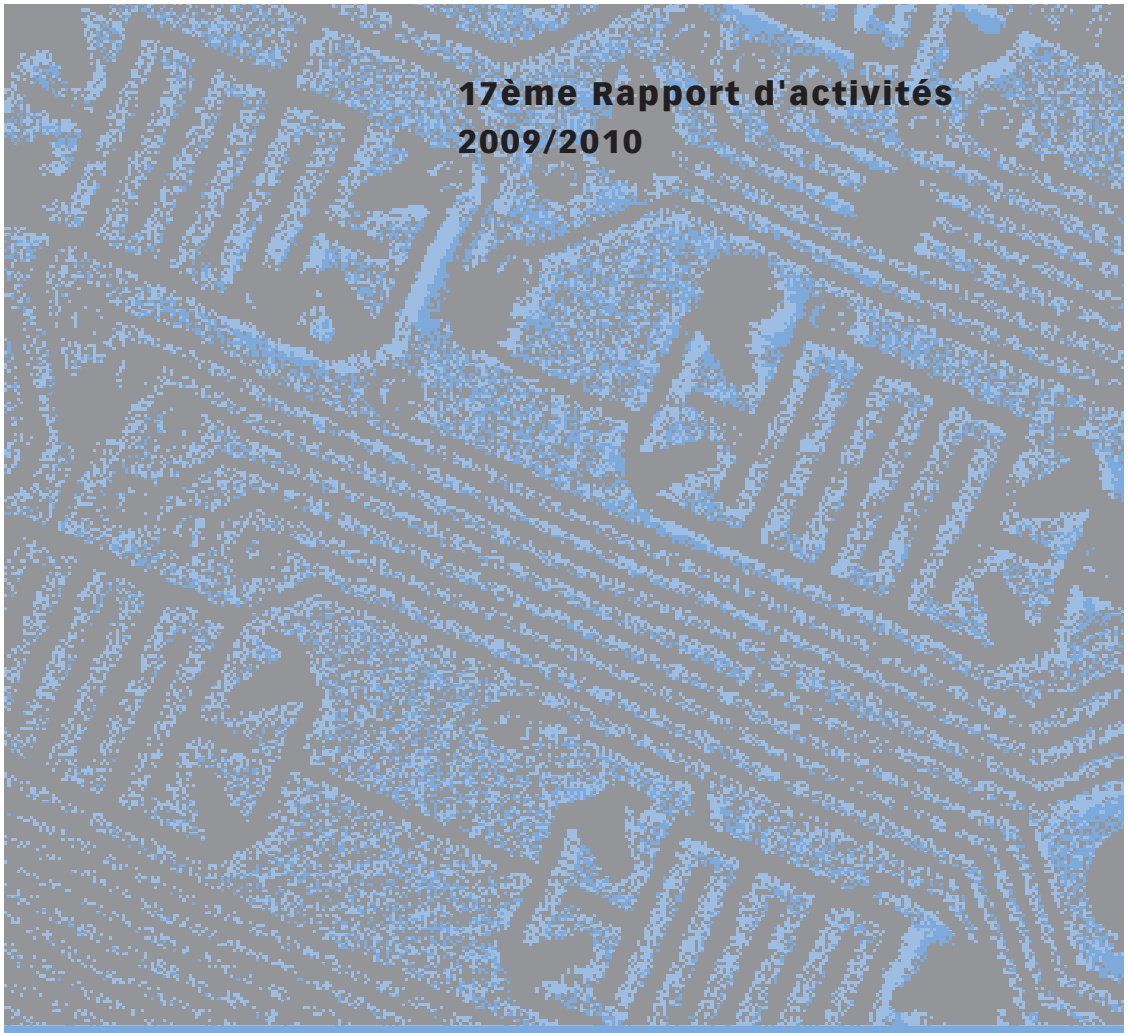


17ème Rapport d'activités 2009/2010

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2009/2010 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 au Conseil fédéral un rapport sur son activité (art. 30 LPD). Le présent rapport couvre la période du 1er avril 2009 au 31 mars 2010.

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. 410.017.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Ruée vers l'or sur Internet – la fin de la sphère privée?

Il ne se passe guère de semaine sans que des géants de la Toile comme Google ou Facebook ne lancent de nouveaux produits ou services, aussi novateurs qu'impressionnants. Ceux-ci fonctionnent toujours selon le même modèle: ils sont gratuits, les fournisseurs assurant leurs revenus par le biais de la publicité. Plus le nombre des utilisateurs s'accroît et plus leurs besoins sont analysés de manière ciblée, plus les recettes publicitaires des fournisseurs augmentent. Ces derniers mettent donc tout en œuvre pour rassembler un maximum d'utilisateurs et de possibilités de publicité. Voici quelques exemples récents:

- Facebook offre un outil permettant à ses membres de synchroniser leurs agendas et leurs carnets d'adresses sur sa plateforme. Mais les contacts ainsi téléchargés sont mis à la disposition non seulement des utilisateurs eux-mêmes, mais aussi de Facebook. Cette société a donc accès à des informations concernant des personnes qui ne sont pas au courant de cette transmission de données et n'y ont pas consenti.
- Google a également depuis peu pénétré le marché lucratif des réseaux sociaux et offre, avec «Google Buzz», aux utilisateurs de Gmail un outil grâce auquel ils peuvent échanger des informations avec des «amis». Un tollé général s'en est suivi. En effet, Google avait structuré les fonctions de base du programme de telle manière que l'ensemble des échanges de courriels entre les 176 millions d'utilisateurs de Gmail qui cliquaient sur cet outil étaient rendus publics.
- Twitter possède désormais un outil de localisation. Avec ce dernier, on peut donc non seulement communiquer ses pensées et ses activités à ses amis («followers»), mais aussi leur indiquer l'endroit où l'on se trouve: les navigateurs permettent de poursuivre les utilisateurs de Twitter pas à pas et d'établir leurs coordonnées. Mis à part le fait que les amis Twitter savent ainsi en tout temps où l'on se trouve, Twitter le sait également et peut cibler sa publicité avec davantage de précision: la personne se tenant tout près d'un magasin de vêtements par exemple recevra alors une offre intéressante par SMS.
- Le téléphone portable «Android», récemment lancé par Google, offre un logiciel de navigation gratuit disposant d'une technique de recherche pointue:

il suffit de dire «Navigue vers l'exposition <Städel Museum> à Lausanne!» et l'appareil nous conduit virtuellement à la Fondation de l'Hermitage. Inutile de préciser que cet outil génère d'énormes possibilités de publicité.

- Avec «Goggle», Google s'essaie à la reconnaissance faciale automatique grâce à un logiciel pour téléphone portable. Un moteur de recherche permet de déterminer si la personne photographiée figure déjà dans une banque de données accessible sur Internet et transmet le résultat de ses recherches sur le portable.

Le téléphone portable muni de la fonction de localisation permettra en tout lieu de recevoir des informations sur l'endroit où l'on se trouve, de repérer les curiosités touristiques, de retrouver des amis et d'identifier des personnes. Ainsi, le monde réel devient en quelque sorte une interface-utilisateur numérique qui permet d'accéder à des données en tout temps et en tout lieu. Autrefois, on allait «sur Internet», dans cet espace virtuel que l'on nomme le cyberespace. Dorénavant, le réseau est partout: c'est l'«Outernet», selon les termes du spécialiste des tendances Nils Müller.

L'exploitation des données de millions d'utilisateurs est une véritable manne pour les géants de la Toile. Ils connaissent les préférences de leurs clients, savent où ils se trouvent et se déplacent, avec qui ils ont des contacts, ce qui les intéresse et ce qu'ils pensent. Parmi toutes ces données, les logiciels d'analyse actuels, extrêmement efficaces, détectent des algorithmes qui permettent d'établir des profils de la personnalité et de consommation frisant la perfection. La publicité est ainsi ciblée en fonction de l'utilisateur (lieu, heure, produit et personne) avec un degré de précision jusqu'ici jamais atteint. Rien d'étonnant à ce que les supports publicitaires traditionnels du monde entier, surtout dans la presse, craignent pour leurs recettes: aux Etats-Unis, la publicité en ligne a déjà dépassé la publicité imprimée. On ne s'étonnera pas davantage d'apprendre que les commissions de l'OCDE et les gardiens de la concurrence s'inquiètent de la position dominante des géants de la Toile. Même aux Etats-Unis, certains organes nationaux commencent à se pencher sur cette problématique.

Cette évolution soulève une question intéressante: comment ces nouveaux produits vont-ils influencer notre comportement? Lorsque des algorithmes influent de plus en plus sur notre vie, nous disent ce que nous sommes et ce que nous devrions faire, l'autodétermination en tant qu'essence de notre modèle social libéral est remis en question. Des études sont en cours concernant les répercussions, sur les mécanismes démocratiques de décision, de nos perceptions et de nos prises de décision lorsque celles-ci sont régies par des algorithmes. Je suis impatient d'en connaître les résultats.

Face à ce genre d'évolutions, rien de sert de verser dans le pessimisme culturel et de voir tout en noir, même si l'on ne peut nier qu'il s'agit là d'un grand défi pour tous ceux qui se sentent tenus de veiller à la protection de la sphère privée. Ce n'est pas seulement la protection des données qui est concernée, mais bien la société toute entière:

En premier lieu, les utilisateurs: Ceux-ci doivent tout d'abord rester conscients que les informations personnelles qu'ils communiquent ont de la valeur. Il leur appartient ensuite de décider si l'offre qui leur est faite mérite que ces données soient diffusées sur Internet. La responsabilité individuelle implique avant tout de lire ce qui est imprimé en tout petits caractères et s'assurer des informations que l'on veut vraiment communiquer, en sachant bien qu'elles permettent d'établir des profils de la personnalité très détaillés. Les utilisateurs doivent aussi savoir qu'ils ne peuvent pas mettre en réseau des informations concernant amis et connaissances (par exemple des photos prises lors de fêtes de famille ou de courses d'école) sans le consentement de toutes les personnes concernées.

Le législateur est également mis à contribution: Celui-ci doit lui aussi savoir que toutes ces offres Internet ont pour objectif premier de rassembler un maximum de données personnelles, afin de générer le plus grand nombre possible de recettes publicitaires. Raison pour laquelle les fonctions de base de ces produits ne sont pas axées sur la protection de la sphère privée. Dans l'optique d'une protection de la personnalité bien pensée, on ne peut arriver à la situation dans laquelle la personne souhaitant protéger sa sphère privée doit se protéger elle-même. C'est exactement le contraire: tout fournisseur doit être tenu, de par la loi, de choisir la technologie et les fonctions qui garantissent le mieux la sphère privée. Les utilisateurs qui ne veulent pas de cette protection sont libres d'y renoncer, mais ils doivent accomplir eux-mêmes les démarches nécessaires pour ce faire et adapter les fonctions de base de leurs comptes. Dans ce contexte, il est important de souligner qu'à elles seules, les réglementations nationales ne pourront résoudre le problème. Des mesures à l'échelon international s'imposent également.

Les médias et les écoles sont aussi concernés: Pour que les utilisateurs soient en mesure d'utiliser les nouvelles techniques en étant conscients de leur responsabilité, il faut leur fournir les informations et explications nécessaires. Ici, l'école a pour mission de donner aux enfants et aux jeunes une base suffisamment solide pour qu'ils prennent conscience de la valeur de leur sphère privée. Chaque niveau de la formation doit aborder cette réalité que sont les nouveaux moyens de communication et montrer comment s'en servir.

Enfin, les fournisseurs de ce type de services sont bien entendu eux aussi largement concernés: Dans l'intérêt de leur propre image, il devrait leur tenir à cœur de ne mettre sur le marché que des produits respectueux de la protection des données de sorte que l'utilisateur ne soit pas encore obligé prendre des mesures supplémentaires dans ce sens. Mais je ne me fais aucune illusion à cet égard: seule la pression de l'opinion publique amènera les grands fournisseurs sur le chemin de la vertu.

Dans le cas de Google Street View, qui nous a fort occupés au cours de l'année écoulée et qui nous occupera encore, nous touchons là au point essentiel: jusqu'à quel degré de perfection un produit doit-il aller du point de vue de la protection de la sphère privée? Est-il juste qu'une personne doive intervenir sur le réseau lorsque la protection offerte ne lui suffit pas? Cette question de fond trouvera peut-être une réponse auprès du Tribunal administratif fédéral cette année encore. L'arrêt attendu sera aussi déterminant pour d'autres fournisseurs de services sur Internet.

Même si de plus en plus de personnes semblent se résigner à l'abandon quasi total du «privé», la conclusion que le chef de Google, Eric Schmidt, a récemment tirée ne devrait pas – et pour longtemps encore – rassembler la majorité des suffrages, du moins nous l'espérons. Selon ses propres termes, «Lorsqu'il y a une chose que vous ne voulez pas que n'importe qui apprenne, peut-être ne devriez-vous pas la faire du tout». Une réflexion qui va tout à fait dans le sens des déclarations du fondateur de Facebook, Mark Zuckerberg, selon lequel la sphère privée serait une notion dépassée.

Or les utilisateurs montrent tous les jours qu'ils n'entendent pas que leurs données personnelles soient considérées avec désinvolture. Ils protestent, ils bloguent, ils constituent des groupes d'intérêts et obtiennent des améliorations. En notre qualité d'autorité de protection des données, nous ne pouvons que soutenir entièrement cette tendance.

Hanspeter Thür

Répertoire des abréviations

ACC	Autorité de contrôle commune
AFC	Administration fédérale des contributions
AMA	Agence mondiale antidopage
ARE	Office fédéral du développement territorial
ATF	Arrêt du Tribunal fédéral
ChF	Chancellerie fédérale
CC	Code civil
CFPP	Commission fédérale des prestations générales et des principes
CO	Code des obligations
CP	Code pénal suisse
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFE	Département fédéral de l'économie
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
ESPA	Enquête suisse sur la population active
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
FIV	Fécondation in vitro
GEWA	Système de traitement des données en matière de lutte contre le blanchiment d'argent
IDE	Numéro d'identification des entreprises
IDHEAP	Institut de hautes études en administration publique

ISIS	Système de traitement des données relatives à la protection de l'Etat
IVI	Institut de Virologie et d'Immunoprophylaxie
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAA	Loi fédérale sur l'assurance-accidents
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LCD	Loi sur la concurrence déloyale
LIDE	Loi fédérale sur le numéro d'identification des entreprises
LOGA	Loi sur l'organisation du gouvernement et de l'administration
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi fédérale sur la protection des données
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
LRH	Loi fédérale relative à la recherche sur l'être humain
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
LTVA	Loi fédérale régissant la taxe sur la valeur ajoutée
N-SIS	Partie nationale du Système d'information Schengen
OCDE	Organisation de coopération et de développement économiques
OCPD	Ordonnance sur les certifications en matière de protection des données
ODM	Office fédéral des migrations
OFAC	Office fédéral de l'aviation civile
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFCOM	Office fédéral de la communication

OFEN	Office fédéral de l'énergie
OFEV	Office fédéral de l'environnement
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFROU	Office fédéral des routes
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OPGA	Ordonnance sur la partie générale du droit des assurances sociales
OPrI	Ordonnance concernant la protection des informations de la Confédération
ORTV	Ordonnance fédérale sur la radio et la télévision
OTVA	Ordonnance régissant la taxe sur la valeur ajoutée
PFPDT	Préposé fédéral à la protection des données et à la transparence
PGP	Pretty Good Privacy
PJF	Police judiciaire fédérale
RFID	Radio Frequency Identification
RSA	Rivest-Shamir-Adelman (algorithme)
S/MIME	Secure / Multipurpose Internet Mail Extensions
SAS	Service d'accréditation suisse
SIRENE	Supplementary Information Request at the National Entry
SIS	Système d'information Schengen
SUVA	Caisse nationale suisse d'assurance en cas d'accidents
SYMIC	Système d'information central sur la migration
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
USIC	Unité de stratégie informatique de la Confédération

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Certification de systèmes de gestion de la protection des données: accréditations

Le Service d'accréditation suisse (SAS) a accrédité les premières entreprises privées suisses pour la certification de l'organisation et de la procédure en matière de protection des données. Nous avons pu l'accompagner dans ce processus. Les noms des entreprises accréditées sont publiés sur le site web du SAS.

Depuis que nos directives concernant les exigences minimales envers un système de gestion de la protection des données (certification de l'organisation et de la procédure) sont entrées en vigueur le 1er septembre 2008, les entreprises privées ont également la possibilité de se faire accréditer. La responsabilité de l'accréditation incombe au Service d'accréditation suisse (SAS) qui doit nous associer pour la procédure d'accréditation. Nous avons donc accompagné le SAS pour ces accréditations, non seulement lors des examens sur place, mais également lors des audits sous surveillance. Dans cette phase, notre rôle se limitait à observer et à répondre aux éventuelles questions du SAS ou de l'experte. Ceci nous a permis de recueillir nos premières impressions sur l'accréditation ainsi que sur la certification dans la pratique. Ces expériences nous seront utiles dans le cadre de notre fonction de surveillance, qui subsiste également pour les entreprises certifiées. Nous avons en outre constaté à quel point il est important de définir clairement l'objet à certifier (c.-à-d. l'étendue des procédures de traitement à certifier).

Les noms des entreprises accréditées sont publiés sur le site web du SAS (www.sas.ch, sous «Organismes accrédités»).

1.1.2 Certification de produits: quo vadis?

Nous avons, par l'intermédiaire de l'Office fédéral de la justice, déposé une demande auprès du Conseil fédéral pour qu'il prolonge le délai qui nous est imparti l'ordonnance sur les certifications en matière de protection de données pour l'émission des directives.

Les difficultés déjà mentionnées dans notre dernier rapport d'activités (cf. notre 16e rapport d'activités 2008/2009, ch. 1.1.1) concernant l'édiction des directives pour la

certification de produits n'ont que partiellement pu être résolues. Nous avons donc décidé d'accorder plus de temps à la recherche de solutions optimales et déposé une demande auprès du Conseil fédéral pour qu'il prolonge le délai qui nous est imparti à l'art. 5 al. 3 de l'ordonnance sur les certifications en matière de protection de données (OCPD) pour l'émission des directives.

En février 2010, nous avons invité les personnes intéressées à une séance d'information pour rendre compte de l'avancement de nos travaux. Nous avons ensuite mis sur pied un groupe de travail et nous sommes confiants que nous réussirons à édicter ces directives une fois ces travaux achevés.

1.1.3 Recensement 2010

En 2010, grâce à l'harmonisation des registres, le recensement de la population sera pour la première fois effectué selon le nouveau système. Avec ce dernier, de gros volumes de données seront collectés chaque année auprès des citoyennes et citoyens. Nous avons accompagné plusieurs projets et nous avons pu constater que les acteurs sont en principe sensibilisés aux questions de protection des données.

Le recensement 2010 sera pour la première fois effectué selon un système rendu possible par l'harmonisation des registres. Ce dernier consiste à collecter les données de base des registres cantonaux des habitants, des principaux registres fédéraux et du registre fédéral des bâtiments et des logements. En plus d'une enquête par sondage effectuée auprès de 200'000 citoyennes et citoyens, une enquête thématique sera également effectuée, dans le cadre de laquelle 10'000 à 40'000 personnes seront interrogées sur leur comportement en matière de mobilité et de déplacement. Finalement, diverses enquêtes plus petites, appelées «relevés Omnibus», seront organisées par l'Office fédéral de la statistique (OFS) sur des thèmes choisis. Il est important que les citoyens concernés sachent que le recensement n'est pas un gros projet unique de statistique qui n'a lieu que tous les 10 ans. A l'avenir, l'OFS collectera et traitera chaque année de gros volumes de données dans le cadre du recensement.

Les relevés selon le nouveau système n'entreront dans leur phase productive qu'à partir du milieu de 2010. Nous avons accompagné l'OFS lors de ces travaux et nous avons pris position sur divers concepts qui touchent à la protection des données. Dans la mesure où il nous est possible de l'apprécier, nos suggestions ont été mises en œuvre. Nous continuerons à accompagner le recensement de très près et avons déjà prévu les contrôles correspondants.

Dans le cadre des travaux préparatifs au recensement, la Poste agit en qualité de prestataire privé pour l'attribution initiale de l'identificateur de logement. Ce sont surtout de grandes communes urbaines ainsi que certains cantons qui ont bénéficié de cette prestation. Celle-ci a soulevé plusieurs problèmes au niveau de la protection des données; ceux-ci n'ont pas été faciles à résoudre en raison du partage des compétences entre la Confédération et les cantons. Nous avons conseillé la Poste en conséquence et l'avons, lorsque cela était nécessaire, renvoyée aux organes compétents.

A part la Poste, divers autres acteurs participeront au recensement. L'OFS a mis au concours et adjugé les mandats correspondants, tandis que nous avons contrôlé les contrats quant aux clauses de protection des données. Dans le cadre de cet examen, nous avons rendu l'OFS attentif au fait qu'il devait contrôler l'application des dispositions en matière de protection des données. Un autre problème qui était déjà apparu lors du dernier recensement est le respect du principe de finalité, qui interdit aux prestataires externes d'utiliser les données collectées à des fins statistiques lors du recensement pour d'autres usages. Nous allons suivre ces développements dans le cadre de notre activité de surveillance.

1.1.4 ESPA – Enquête téléphonique statistique de la Confédération

En automne 2009, les personnes physiques ont été pour la première fois obligées de répondre à ESPA, l'enquête suisse sur la population active. Cette obligation ainsi que le fait que l'enquête a été effectuée par un institut privé, mandaté par l'Office fédéral de la statistique (OFS), a soulevé une vague de protestations et déconcerté beaucoup de citoyennes et citoyens. Nous avons conseillé l'OFS dans cette affaire et avons pris position à ce sujet.

Depuis octobre 2009, les citoyennes et citoyens qui sont interrogés dans le cadre de l'enquête ESPA sont tenus de fournir une réponse. Cette enquête permet de récolter des informations sur les conditions de travail, les répercussions de la libre circulation des personnes et le taux de travailleurs à faible revenu («working poor») en Suisse.

Ce n'est pas seulement l'introduction de l'obligation de répondre pour les citoyens qui a désorienté les personnes concernées, mais également le fait que les appels téléphoniques ont été effectués par un institut privé mandaté par l'Office fédéral de la statistique (OFS). Cette incertitude a encore été renforcée par des articles de presse qui évoquaient de grosses amendes pour les personnes qui refuseraient de répondre.

Nous avons soutenu l'OFS dans le cadre de leur activité de conseil aux citoyens inquiets et avons proposé diverses mesures devant permettre de restaurer la confiance de la population en un traitement des données qui soit conforme aux exigences de la protection des données. Pour ce faire, nous avons mis l'accent sur une authentification plus claire de l'institut qui effectuait les enquêtes. Suite à notre proposition, l'OFS a ajouté un code à la lettre d'information que les personnes sélectionnées pour l'enquête recevaient préalablement à l'enquête. Ceci a permis au citoyen appelé de demander à la personne de l'institut de lui indiquer le code pour vérifier ainsi qu'il était bien appelé par l'institut autorisé à collecter les données pour l'enquête ESPA.

Dans une prise de position adressée à l'OFS, nous avons relevé que nous considérons la méthode des appels téléphoniques comme plutôt problématique pour une enquête obligatoire. Les nombreuses questions et plaintes qui nous ont été adressées ont clairement montré que celle-ci était ressentie comme une atteinte disproportionnée à la vie privée. Nous saluons les débats parlementaires intervenus à ce sujet lors de la session de printemps 2010. Il est d'ailleurs indéniable que ce type d'enquête téléphonique est utilisé par des entreprises peu sérieuses dans le but de se procurer des données personnelles. C'est pourquoi nous déconseillons en principe de communiquer à la légère des données personnelles au téléphone sans vérifier la finalité de la collecte de données. Nous sommes bien conscients qu'une telle vérification demande beaucoup de circonspection et d'aptitude à s'imposer de la part des citoyens. Nous nous engageons donc pour que l'OFS n'applique plus la méthode des appels téléphoniques pour les futures enquêtes obligatoires.

1.1.5 La nouvelle loi relative à la recherche sur l'être humain

Le projet de loi relatif à la recherche sur l'être humain a été adopté en octobre 2009 par le Conseil fédéral, puis déféré au Parlement pour qu'il en débatte. Nous avons eu l'occasion, dans le cadre d'une consultation des offices, de prendre préalablement position. Le projet de loi prévoit une clause échappatoire pour les chercheurs travaillant dans le domaine de la réutilisation d'échantillons biologiques et de données personnelles relatives à la santé d'une personne. Nous considérons cela comme hautement problématique.

Dans le cadre de la consultation des offices, nous avons pris position sur le projet de la loi fédérale relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH). La loi est censée combler une lacune dans la législation suisse en matière de santé. Nous saluons ces efforts, surtout parce que le nouveau projet attache une importance particulière à la protection de la dignité humaine. Malheu-

reusement, le projet de loi ainsi que l'article constitutionnel sur lequel il repose et sur lequel nous avons été appelés à voter au printemps 2010 ne réglemente que le traitement des données dans le cadre de la recherche biologique et médicale. Les autres domaines de recherche sur l'être humain, tels que la recherche psychosociale, en sont exceptés.

Dans notre prise de position, nous avons rendu l'Office fédéral de la santé publique (OFSP) attentif à divers problèmes en matière de protection des données. Nous abordons ici plus en détail deux des points concernés.

D'une part, les tâches de la Commission d'experts du secret professionnel en matière de recherche médicale sont déléguées aux commissions cantonales d'éthique. L'autorisation de la Commission d'experts a régulièrement été assortie de charges en matière de protection des données, dont nous avons ponctuellement contrôlé l'application. Nous avons assisté aux séances de la Commission d'experts en tant que conseiller sans droit de vote. Une nouvelle disposition exige maintenant que les commissions d'éthique soient constituées de manière qu'elles disposent des compétences professionnelles et de l'expérience nécessaire pour l'accomplissement de leurs tâches. Le Conseil fédéral a la compétence d'édicter des prescriptions à ce sujet. Nous avons alors insisté sur le fait que les membres des commissions d'éthique devraient dorénavant avoir également des connaissances de la législation sur la protection des données, afin que celle-ci soit prise en compte lors de l'élaboration des projets par les chercheurs.

D'autre part, une clause échappatoire (escape clause) est créée pour la réutilisation d'échantillons biologiques et de données relatives à la santé d'une personne. Cela signifie que les chercheurs dans ce domaine ne doivent plus respecter les principes généraux de la protection des données, qui exigent que l'on demande le consentement de la personne concernée après l'avoir informée du but du traitement de données. Cette autorisation générale pour les chercheurs est extrêmement inquiétante du point de vue de la protection des données; à notre avis, le projet de loi a trop fortement tenu compte des propres intérêts du secteur économique concerné.

1.1.6 Procédure de consultation relative à la loi fédérale sur le numéro d'identification des entreprises

Lors des diverses procédures de consultation, nous avons souligné les possibilités de surveillance et d'atteintes à la personnalité inhérentes à l'utilisation du numéro d'identification des entreprises (IDE) dans le domaine Business to Business, en particulier le risque de profilage. De plus, nous avons recommandé d'une part que l'utilisation de l'IDE dans ce domaine soit interdite ou à tout le moins limitée, d'autre part que l'Office fédéral sur la statistique ne publie l'IDE sur Internet que si la personne concernée a donné son consentement.

Comme nous l'avons déjà mentionné dans notre 16e rapport d'activités 2008/2009 (ch. 1.1.4), l'examen du projet de loi fédérale sur le numéro d'identification des entreprises (LIDE) démontre que les utilisations de ce numéro pour faciliter les échanges d'informations entre les entreprises et l'administration (Business to Government – B2G) et à l'intérieur de l'administration (Government to Government – G2G) répondent au principe de proportionnalité, mais qu'en revanche l'utilisation complémentaire entre les différentes entreprises (Business to Business – B2B) augmente fortement les possibilités de surveillance et d'atteintes à la vie privée, en permettant notamment le profilage. Or ces risques ne sont pas suffisamment pris en compte dans le projet de loi. Aussi, nous sommes d'avis que l'utilisation de l'IDE pour les applications entre entreprises devrait être interdite, ou à tout le moins limitée.

Dans l'optique d'utilisations de l'IDE non seulement dans les domaines B2G et G2G mais également B2B, la loi devrait prévoir que le Conseil fédéral fixe les limites d'utilisation dans ce domaine. De plus, les limitations mentionnées dans le rapport relatif aux résultats de la procédure de consultation (interdiction d'utiliser l'IDE de manière abusive, à des fins publicitaire ou de marketing ou interdiction de transmettre l'IDE à l'étranger), devraient être reprises au niveau de l'ordonnance.

La première version du projet prévoyait la publication sur Internet de l'IDE par l'Office fédéral de la statistique (OFS), à l'exception des cas où la personne concernée s'y est opposée (principe d'opt-out). Suite à nos remarques concernant les modalités de publication, l'OFS a modifié son projet de loi, de sorte que l'IDE ne peut être publiée sur Internet que si la personne concernée a donné son consentement (principe d'opt-in). Par ailleurs, nous estimons que la portée du consentement au sens de l'art. 13 al. 1 du projet de loi actuel est trop générale et que cette disposition devrait être modifiée afin de limiter le consentement au cas d'espèce.

1.2 Protection des données – Questions d'ordre géneral

1.2.1 Enregistrements vidéo effectués par des drones

La protection des données doit également être respectée lors d'enregistrements vidéo effectués depuis des drones ou autres aéronefs, dans les cas où les enregistrements permettent d'identifier des personnes. Nous avons à ce sujet fixé plusieurs critères qui doivent être examinés de cas en cas.

L'Office fédéral de l'aviation civile (OFAC) nous a demandé quels étaient les critères devant être respectés en matière de protection des données lors d'enregistrements vidéo effectués depuis des aéronefs. Il est difficile de fixer des critères généraux, car il faut toujours examiner le cas concret. En nous basant sur notre feuillet thématique «Vidéosurveillance effectuée par des personnes privées» (voir notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Vidéosurveillance), nous avons pu cependant retenir les points suivants:

Dès lors que les images filmées se rapportent à des personnes identifiables, on doit en tout premier lieu déterminer si les images sont utilisées par une personne physique uniquement pour son usage personnel et ne sont pas transmises à des personnes extérieures à la famille ou aux proches, ni publiées. Dans ces cas, la LPD n'est pas applicable. Par contre, si le traitement des images dépasse l'usage personnel – qui doit être défini de manière très restreinte – p. ex. par une publication sur Internet, les personnes apparaissant sur les images doivent être rendues méconnaissables par des moyens techniques.

Si une personne privée effectue des prises de vue depuis un aéronef (p. ex. un drone) et que les images prises ne sont pas destinées exclusivement à son usage personnel, les règles suivantes sont applicables: toute personne privée qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Une atteinte à la personnalité est contraire à la loi si elle n'est pas justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public, ou par la loi. On ne peut guère partir de l'idée qu'une personne privée puisse se fonder sur une base légale pour légitimer des prises de vue depuis un aéronef. Elle doit donc avoir le consentement de la personne concernée ou pouvoir faire valoir un intérêt privé ou public prépondérant.

La personne privée doit en outre respecter les principes généraux de la protection des données: ainsi, les données personnelles doivent être collectées de manière licite; leur traitement doit respecter les règles de la bonne foi et être proportionnel; les données

personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. La collecte de données personnelles et en particulier le but de leur traitement doivent être reconnaissables pour la personne concernée. Lorsque le consentement de la personne concernée est requis pour justifier le traitement de données personnelles, celui-ci n'est valable que s'il a été donné de plein gré (et pour les données personnelles sensibles, de manière explicite) après une information suffisante. Des données personnelles ne peuvent pas être communiquées à l'étranger si ceci risque de constituer une atteinte grave à la personnalité des personnes concernées, notamment parce qu'une protection des données équivalente à celle de la Suisse fait défaut dans les pays destinataires. S'il existe un motif justificatif et si des mesures moins attentatoires ne sont pas possibles, les données devront être supprimées ou anonymisées aussi rapidement que possible.

Comme mentionné, il faut examiner de cas en cas si ces conditions sont respectées. Nous renvoyons ici à notre feuillet thématique «Vidéosurveillance effectuée par des personnes privées» qui, bien qu'il ait été élaboré pour l'utilisation de la vidéosurveillance dans le domaine de la sécurité, peut également être consulté dans ce cas comme notice interprétative.

Lors de l'utilisation de drones à des fins de vidéosurveillance, les points suivants doivent en outre être respectés du point de vue de la protection des données:

- La vidéosurveillance – avec ou sans enregistrement – de personnes identifiables, n'est autorisée que s'il existe un motif justificatif. En l'espèce, ce peut être le consentement de la personne concernée ou éventuellement un intérêt public ou privé prépondérant.

  Exemple n° 1: l'engagement de drones pour prendre des images d'un site archéologique.

  Exemple n° 2: les drones sont utilisés à des fins non personnelles, p. ex. pour une planification, et les résultats sont publiés de manière que les personnes ne puissent pas être identifiées.

- L'autorisation de l'OFAC pour de telles prises de vue devrait mentionner de manière aussi précise que possible à quelles fins la vidéosurveillance avec ou sans enregistrement est effectuée. Les prises de vue doivent être utilisées uniquement dans le but indiqué (principe de la finalité). Il va de soi que les prises de vue ne peuvent être effectuées que si elles sont nécessaires et appropriées pour atteindre le but visé. Si le même but peut être atteint avec des mesures moins attentatoires à la personnalité, on renoncera aux prises de vue (principe de la proportionnalité).

Exemple: lors de prises de vues effectuées sur un chantier de construction ou un site archéologique, le champ de vision de la caméra vidéo ne peut inclure des personnes identifiables que si ces dernières ont donné leur consentement ou si les drones sont utilisés à des fins non personnelles et que les résultats sont publiés sous forme anonymisée.

- La surveillance vidéo doit être reconnaissable pour les personnes concernées, p. ex. par un panneau indicateur ou par la visibilité de la caméra (principe de transparence).

  Exemple: dans un bâtiment surveillé par une société de surveillance privée, un pictogramme indique qu'une vidéosurveillance est effectuée par des drones.

- Si les images prises sont liées à un fichier, il doit en outre être indiqué auprès de qui la personne concernée peut faire valoir son droit d'accès.

  Exemple: à côté du pictogramme figure une mention avec le nom, l'adresse et le numéro de téléphone du service qui traite les demandes d'accès.

- Les données personnelles doivent être protégées par des mesures techniques et organisationnelles appropriées contre tout accès ou traitement non autorisé (sécurité des données).

  Exemple: le support de données qui contient les images est conservé dans une armoire fermée à clé qui n'est accessible qu'aux personnes autorisées.

- Les drones doivent être engagés de manière à ce que le champ de vision de la caméra n'embrasse que les images qui sont absolument nécessaires pour atteindre le but visé (principe de proportionnalité).

  Exemple: lors des prises de vue du chantier, le drone ne filme que le chantier même et non pas les bâtiments voisins.

- Les enregistrements incluant des personnes identifiables ne doivent pas être transmises à des tiers, sauf dans les cas prévus ou autorisés par la loi, tels que des demandes émanant de juges (principe de finalité).

  Exemple: un juge demande qu'on lui fournisse les images dans le cadre d'une procédure pénale en cours.

- Les images enregistrées doivent être supprimées ou anonymisées dans un délai particulièrement bref. La durée de conservation dépend du but poursuivi; il faut cependant partir du principe qu'une durée d'une semaine au maximum devrait être suffisante dans la majorité des cas.

  Exemple: les images prises sur le chantier sont anonymisées dans les 24 heures.

- Les demandeurs d'autorisation devraient si possible également être rendus attentifs aux éventuelles conséquences pénales (p.ex. violation de domicile).

1.2.2 Systèmes de reconnaissance biométrique: Suivi du contrôle au centre sportif KSS

Le Tribunal administratif fédéral considère que le stockage des données biométriques dans une base de données centralisée dans le cadre du contrôle d'accès à un centre de sport et de détente représente une atteinte disproportionnée à la personnalité des personnes concernées.

Suite au refus du centre sportif KSS à Schaffhouse de suivre notre recommandation relative à la décentralisation des données biométriques (Match on card) (voir notre 16e rapport d'activité 2008/2009, ch. 1.2.4), nous avons porté le cas devant Tribunal administratif fédéral (TAF).

Dans son arrêt du 4 août 2009 (A-3908/2008), le TAF a admis notre action et apporté plusieurs précisions concernant les questions de protection des données dans le cadre de la mise en œuvre de systèmes de reconnaissance biométrique. Il a en particulier précisé que les données dérivées (templates), en l'occurrence les réductions numérisées d'une empreinte digitale brute, constituent des données personnelles au sens de la LPD et que dans la mesure où des données personnelles sont stockées dans un fichier centralisé, les personnes concernées perdent totalement le contrôle de l'utilisation qui peut être faite de leurs données personnelles. En conséquence, le TAF est arrivé à la conclusion que le stockage des données biométriques dans un fichier centralisé dans le cadre du contrôle d'accès à un centre de sport et de détente représente une atteinte disproportionnée à la personnalité des personnes concernées. De plus, le Tribunal relève que l'atteinte à la personnalité n'est justifiée ni par le consentement des personnes concernées (celles-ci ne n'étant pas suffisamment informées et n'étant pas libres de donner leur consentement), ni par un intérêt privé prépondérant.

Par ailleurs, le TAF a estimé que la solution technique que nous avions proposée, à savoir un système décentralisé match on card, est adéquate, tout en laissant la porte ouverte à d'autres solutions techniques pour autant qu'elles répondent aux exigences de la protection des données. Le Tribunal rappelle enfin que le centre sportif KSS est cependant libre de renoncer de lui-même à utiliser un système biométrique.

Notre demande au TAF est reproduite, en version allemande, à l'annexe 4.1.8. Ce document peut en outre être consulté sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des données – Actions en justice.

1.2.3 Vision locale concernant l'installation d'un système de contrôle d'accès dans un domaine skiable

Les systèmes de contrôle d'accès dans les domaines skiables doivent respecter la LPD. Conformément au principe de proportionnalité, l'écran avec affichage des données des titulaires d'abonnements ne doit pas être orienté vers les autres usagers, mais uniquement vers le personnel chargé de contrôler la validité des abonnements. Suite à une plainte d'un particulier à ce sujet, les exploitants d'une station de ski ont accepté notre demande de tourner le moniteur de façon à ne plus être visible pour les autres usagers.

Comme nous avons déjà eu l'occasion de le présenter (cf. notre 14e rapport d'activités 2006/2007, ch. 1.2.8), les systèmes de contrôle d'accès dans les domaines skiables doivent respecter les exigences de la loi sur la protection des données. Conformément au principe de proportionnalité, seules les personnes chargées de vérifier la validité des abonnements et l'identité de leurs détenteurs peuvent prendre connaissance des données personnelles contenues dans un abonnement. L'affichage public de la photo, des nom et prénom ou encore de la date de naissance des titulaires d'abonnement n'est pas conforme aux principes de la protection des données. L'écran avec l'affichage des données ne doit par conséquent pas être orienté vers de tierces personnes, en l'occurrence les autres usagers.

Suite à une plainte d'un particulier, nous avons, dans le cadre de nos tâches de surveillance, pris contact avec les exploitants du domaine skiable concerné. Nous leur avons expliqué la situation juridique en la matière et les avons priés de prendre position et de nous indiquer les mesures prises pour la prochaine saison de ski. Les responsables de l'installation ont accueilli favorablement notre demande en nous répondant qu'ils prendraient les mesures nécessaires pour respecter la sphère privée de leurs clients. Au début de la saison hivernale, les responsables du domaine skiable

nous ont cependant indiqué qu'ils avaient renoncé à mettre le moniteur en service et nous ont invités à venir examiner le système sur place. En février 2009, nous avons répondu à cette invitation. Au moment de la vision locale, nous avons pu constater que le moniteur (désactivé) était dirigé en direction de la file d'attente, qu'il était donc directement visible pour les autres usagers. Nous avons accepté la proposition de tourner le moniteur en direction des télécabines, de façon que le personnel placé près des télécabines puisse vérifier l'identité des détenteurs d'un abonnement (notamment lorsque personne ne se trouve dans la cabine de contrôle). Les autres usagers auraient certes la possibilité d'apercevoir à un moment ou à un autre l'écran de contrôle, mais ceci paraît tolérable au regard de l'atteinte minime à la personnalité.

Suite à notre vision locale, nous avons écrit à la société Skidata SA, fournisseur du système d'accès, pour la rendre attentive à cette problématique. Celle-ci nous a indiqué que dans le cadre de ses activités de conseil, elle informerait ses clients de la situation juridique en la matière.

1.2.4 Activités de surveillance de la société Securitas

Dans le cadre des activités de surveillance de la société Securitas SA, nous avons entrepris des investigations dans les limites de nos compétences de contrôle, en particulier en ce qui concerne les activités visant le groupe Attac sur mandat de la société Nestlé SA et celles qui auraient visé le Groupe anti-répression Lausanne. Ne disposant pas de moyens coercitifs tels que ceux à disposition de juges civils ou pénaux, nous nous sommes focalisés sur l'obligation d'annoncer des fichiers en respect de la loi sur la protection des données. L'examen de ces cas a en outre démontré que pour garantir les droits des personnes concernées, les activités de recherches de renseignements effectuées par des entreprises privées doivent être régies par des normes légales.

En juin 2008, l'avocat du groupe Attac a requis notre intervention dans le cas de la surveillance du groupe Attac par la société Securitas SA sur mandat de la société Nestlé SA. Afin d'établir les faits, nous avons adressé aux sociétés Securitas et Nestlé des questions relatives aux traitements de données personnelles effectués dans le cadre de la surveillance d'Attac. Notre demande concernait notamment les motifs justifiant une telle surveillance, la collecte des données concernant les membres d'Attac, le traitement de ces données au sein des sociétés Securitas et Nestlé, la conservation et la communication des données en question. Après avoir constaté que les deux sociétés susmentionnées n'avaient déclaré aucun fichier auprès de notre autorité, nous leur avons également demandé d'annoncer, le cas échéant, leurs fichiers.

L'avocat d'Attac affirmait que Securitas et Nestlé avaient violé le devoir d'informer les personnes concernées lors de la collecte de données sensibles ou de profils de la personnalité et l'obligation de déclarer les fichiers. Sur la base des pièces produites par Nestlé et Securitas, la collecte de données personnelles concernant Attac a cessé à la fin de l'année 2004. Les conclusions du juge d'instruction cantonal vaudois indiquent que cette collecte a cessé fin 2005. L'obligation d'informer les personnes concernées en cas de collecte de données sensibles ou de profils de la personnalité étant en vigueur depuis le 1er janvier 2008, Nestlé et Securitas n'ont pas pu violer cette obligation lors de la collecte des données concernant Attac.

En août 2008, le Groupe anti-répression Lausanne (GAR) nous a demandé de vérifier si les traitements de données liés à la surveillance effectuée par Securitas étaient conformes à la législation fédérale sur la protection des données. En réponse à nos demandes, la société Securitas nous a informés qu'elle n'avait pas traité de données concernant le GAR. Nous avons pris bonne note de ces allégations, ne disposant pas de moyens coercitifs tels que ceux à disposition des juges civils ou pénaux (par exemple la saisie). La LPD délimite en effet clairement le pouvoir d'investigation du PFPDT. Le législateur a ainsi choisi de laisser le soin avant tout aux personnes concernées d'agir elles-mêmes sur le plan civil ou pénal.

En ce qui concerne l'obligation d'annoncer les fichiers auprès de notre autorité, la société Nestlé nous a informés qu'elle avait désigné un conseiller à la protection des données; elle est ainsi déliée de son devoir de déclarer ses fichiers. Securitas nous a indiqué qu'elle ne disposait d'aucun fichier à déclarer conformément à la LPD. Cette question doit encore être examinée.

L'examen des cas Attac et GAR a en outre démontré qu'il est nécessaire d'élaborer des normes régissant les activités de recherches de renseignements effectuées par des entreprises privées (p.ex. sociétés de renseignement et de surveillance, détectives).

1.2.5 Prise de position sur le registre des accidents de la route (Via sicura)

Nous avons pris position sur le projet de registre des accidents de la route. Celui-ci comprend un registre de saisie et un registre d'analyse. Comme des données personnelles sensibles devront également être traitées, un tel traitement doit être prévu par une loi au sens formel.

Dans le cadre de la consultation des offices, nous avons pris position sur la nouvelle ordonnance relative au registre des accidents de la route. Celle-ci doit permettre une saisie harmonisée (moyennant le registre de saisie) et une analyse centrale (moyennant

le registre d'analyse) des accidents de la route. Le registre d'analyse devrait en outre être relié à d'autres systèmes d'information de l'Office fédéral des routes (OFROU). Dans notre prise de position, nous avons en particulier attiré l'attention sur le fait qu'une ordonnance ne suffit pas pour réglementer le registre des accidents de la route; comme des données personnelles sensibles devront également être traitées dans le cadre de ce registre, un tel traitement de données doit être explicitement prévu dans une loi au sens formel.

Nous avons également fait remarquer que les notions de pseudonymisation et d'anonymisation avaient été confondues dans l'ordonnance. Nous avons retenu que les données pseudonymisées doivent – contrairement aux données anonymisées – également être considérées comme des données personnelles au sens de la loi sur la protection des données. Un moyen permettant d'anonymiser des données pseudonymisées est la fonction de hachage. Comme ce processus n'est pas réversible (ou seulement avec des moyens disproportionnés), il est pratiquement impossible de retrouver le pseudonyme et donc d'identifier la personne concernée.

Nous avons participé à une séance organisée par l'OFROU pour discuter du problème de la base légale manquante. Comme il est prévu de créer les bases légales nécessaires pour le registre des accidents de la route lors de la révision de la loi sur la circulation routière (projet Via sicura), il s'agissait principalement de trouver une solution transitoire pour les trois ans à venir, soit jusqu'à l'entrée en vigueur de la révision. Diverses solutions ont été discutées lors de cette réunion. Nous avons pu constater que l'OFROU manifeste un intérêt réel à trouver une solution qui soit conforme aux exigences de la protection des données.

1.2.6 La mise au pilori des chauffards?

Il n'est sans aucun doute pas dans l'intérêt de la protection des données de protéger les chauffards irresponsables. Nous doutons cependant que l'exposition publique soit un moyen de dissuasion adéquat. La souveraineté policière en matière de répression des infractions au code de la route appartient aux cantons. Cela signifie donc que les responsables cantonaux de protection des données sont appelés à concerter leurs actions.

Plusieurs appels ont été lancés ces dernières années demandant qu'il soit permis de publier l'identité de chauffards incorrigibles dans un but dissuasif ou de prévention. Notre intention n'a jamais été de ménager les chauffards pour des raisons de protection de données. On comprend bien que de tels usagers de la route soient considérés

comme une menace et que des accidents tragiques soulèvent le mécontentement. Nous tenons néanmoins à relever que le but primordial des mesures de lutte contre les excès de vitesse est d'éviter que de tels accidents se produisent et que des personnes tierces soient mises en danger. Ces mesures doivent respecter les principes de la proportionnalité et de la finalité. Comme nous l'avons expliqué en détail dans les médias, il est bel et bien légitime de publier (p. ex. sur Internet) les données de chauffards pour permettre de trouver les coupables. Ceci vaut également pour les hooligans et les casseurs.

L'utilisation du pilori comme moyen de dissuasion est cependant un concept qui date du Moyen-Âge et une réintroduction de ce système au 21e siècle nous semble dans le meilleur des cas délicate. Le premier aspect dont il faut tenir compte lors d'une publication est la question de l'égalité devant la loi. Si l'on décide d'exposer publiquement les chauffards, il faut immédiatement se demander pourquoi l'on ne fait pas la même chose pour les autres délinquants. Pourquoi par exemple ne publierait on pas les identités des automobilistes qui ont déjà été poursuivis une fois pour ivresse au volant et qui ont également mis en danger, voire blessé ou tué quelqu'un?

Nous doutons cependant que la mise au pilori ait effectivement un effet dissuasif. Il est bien possible qu'il n'ait pas l'effet voulu, pire, il peut même avoir un effet contraire dans le cas où le chauffard incriminé exploite la publication sur Internet comme un trophée. A ce propos, nous tenons à relever que nombre de chauffards publient eux-mêmes leurs exploits sur Internet, ce qui permet déjà de les identifier comme coupables. Ces exemples montrent clairement qu'une mise au pilori peut effectivement se transformer en un classement.

Une mesure bien plus efficace consisterait à confisquer de manière définitive le véhicule des chauffards impénitents et à leur retirer le permis de conduire pour une durée très longue. De même, les tiers qui mettent délibérément leur véhicule à disposition d'un chauffard devraient également être sévèrement punis. La répression des infractions au code de la route incombe cependant aux polices cantonales. Les responsables cantonaux de la protection des données sont donc appelés à agir de manière coordonnée.

1.2.7 Révision de la loi sur l'encouragement du sport

Dans le cadre de la révision totale de la loi fédérale encourageant la gymnastique et les sports, nous avons proposé deux adaptations législatives constituant une base légale pour les contrôles de dopage, ce qui devrait faciliter l'échange de données entre les différents organes de lutte antidopage. Nos propositions ont été acceptées et intégrées dans la loi. La révision de loi accroît la sécurité du droit pour les sportifs dans le domaine de la lutte contre le dopage.

Jusqu'ici, les contrôles de dopage des sportifs s'effectuaient sur une base plus ou moins volontaire. Les organisateurs de manifestations sportives et les organes de lutte contre le dopage ne pouvaient procéder à des contrôles que si les sportifs déclaraient y consentir. Toutefois, comme les sportifs pouvaient être exclus d'une compétition s'ils refusaient de remettre cette déclaration, on ne pouvait guère parler dans ce contexte d'un consentement libre conformément à la LPD. C'est la raison pour laquelle nous avons suggéré la création d'une base légale qui permet aux organes reconnus de lutte contre le dopage de procéder aux contrôles requis.

Etant donné que dans le sport de haut niveau, les contrôles antidopage sont coordonnés au niveau international et que notamment dans le cas des abus, les données doivent être échangées également au niveau international, il fallait réglementer légalement ce type de transfert de données. Nous avons donc proposé une disposition légale permettant un échange de données au niveau international avec les organes reconnus de lutte contre le dopage (par ex. l'Agence mondiale antidopage) dans le respect des dispositions de la LPD.

1.2.8 Protection des données et dopage

L'Agence mondiale antidopage (AMA) a adopté en 2009 les «Normes internationales pour la protection de la vie privée et des données à caractère personnel». Ces normes permettront d'augmenter le niveau de protection des données au sein de l'AMA et des organismes associées. Néanmoins, elles n'ont pas pour but de mettre en place un niveau de protection des données adéquat conformément à la LPD. Nous avons signalé à l'AMA que d'autres mesures devaient donc être prises en vertu de la LPD avant que des données personnelles venant de Suisse ne soient transmises à l'AMA.

1.2.9 Exonération de payer la redevance pour la radio et la télévision

Conformément à l'ordonnance sur la radio et la télévision, les personnes ayant droit aux prestations de l'AVS ou de l'AI peuvent, à certaines conditions, être exonérées de l'obligation de payer la redevance. Elles sont dans ce cas tenues de fournir à la Billag une preuve adéquate. Dans le cadre de notre activité de surveillance, nous avons constaté que la pratique de la société et en particulier le formulaire de demande prêtaient à confusion. Sur ce formulaire, les personnes concernées transmettaient à la Billag des données dont celle-ci n'avait en général pas besoin. Nous avons alors élaboré avec la société une solution conforme à la protection des données.

L'ordonnance sur la radio et la télévision (ORTV) permet à la Billag de demander aux personnes qui pourraient être exonérées de l'obligation de payer la redevance les informations requises à cet effet. La société Billag n'est pas en droit de demander des informations plus détaillées (notamment des informations sur les montants versés au titre de l'AVS). Il suffit en général que les personnes touchant la rente AVS demandent un certificat auprès de la caisse AVS et le remette à la Billag. Nous avons toutefois eu connaissance d'un cas où une collaboratrice de la Billag a demandé une copie de la décision définitive du droit à des prestations complémentaires. Nous sommes donc intervenus auprès de la Billag. Selon les dires de ses responsables, il s'agissait d'une erreur unique de cette collaboratrice. Nous avons néanmoins constaté que le formulaire de demande prêtait à confusion, en ce sens qu'il demandait au requérant de remettre la décision entrée en force au lieu d'un simple certificat. La Billag nous a promis de modifier le formulaire en conséquence.

1.2.10 L'entraide administrative internationale et l'article 6 LPD

La loi sur la protection des données doit également être respectée en cas d'entraide administrative internationale. Il convient d'abord de vérifier si l'entraide administrative est réglementée par une loi spéciale. Il s'agit d'assurer que la personnalité des personnes concernées n'est pas gravement mise en danger par la communication des données dans un autre pays, notamment parce que ce dernier ne dispose pas d'une législation offrant une protection adéquate. Dans un tel cas, des garanties suffisantes doivent être données. Celles-ci peuvent être fixées dans la clause de protection des données d'un accord ou éventuellement dans une déclaration.

Nous avons participé au groupe de travail interdépartemental sur le thème de l'entraide administrative internationale. La question principale soulevée au niveau de la protection des données était de savoir quel impact l'article 6 LPD a sur l'entraide administrative internationale. C'est la raison pour laquelle nous avons examiné pour le groupe de travail de plus près le thème «Cas particulier LPD – l'article 6 LPD et l'entraide administrative transfrontière». A l'issue de cet examen, nous avons retenu ce qui suit:

En tant que loi transversale, la LPD doit également être respectée lorsque l'entraide administrative est pratiquée au-delà de nos frontières. En principe, les organes fédéraux ne sont autorisés à communiquer des données personnelles que si une base légale suffisante le permet. Une communication de données personnelles sensibles nécessite même une loi au sens formel. Cela signifie qu'il faut, en premier lieu, vérifier si des dispositions spéciales régissant l'entraide administrative existent pour le domaine concerné. Mentionnons ici par souci d'intégralité qu'un accès par procédure d'appel (consultation en ligne) n'est pas considéré comme entraide administrative. Ceci nécessite toujours une base légale.

Lorsque l'entraide administrative est régie par une loi spéciale, il y a lieu d'examiner de cas en cas dans quelle mesure ces dispositions sont en accord ou en conflit avec les prescriptions de la LPD. Même le Tribunal fédéral (TF) a, dans un cas concernant la loi sur les bourses, retenu que l'on ne pouvait pas dire de manière générale – comme pour l'exception prévue à l'art. 2 al. 2 LPD pour l'entraide judiciaire – que la LPD n'était d'emblée pas applicable à l'entraide administrative. Si ce catalogue des exceptions devait – fidèle aux principes «lex specialis derogat legi generali» ou «lex posterior derogat legi priori» – être interprété légèrement au-delà du texte proprement dit, la protection des données perdrait rapidement sa nature de matière transversale avec ses principes uniformes et généraux. Le TF a pourtant relevé que le législateur pouvait, déjà lors de l'élaboration des dispositions légales spéciales, tenir compte de certains principes et exigences prévus par la LPD de façon que ces dispositions de la LPD ne revêtent plus une importance (matérielle) autonome. Si tel est le cas, la LPD peut être consultée de manière subsidiaire afin de définir la marge de manœuvre disponible lors de l'application des dispositions légales spéciales en matière d'entraide administrative. Ceci s'applique en particulier aux principes généraux de la protection des données. Les dispositions légales spéciales doivent donc en principe être prises en compte parallèlement à celles de la LPD (cf. ATF 126 II 126, ou 2A.355/1999). En d'autres termes, le principe est que la LPD reste applicable même en présence de dispositions légales spéciales.

Dans le cas par contre où il n'existe pas de dispositions légales spéciales pour l'entraide administrative, il y a lieu d'examiner si les conditions prévues par la LPD pour

une communication des données sans la présence d'une base légale spéciale sont remplies. Cet examen doit cependant satisfaire à des critères très sévères. Dans tous les cas, les principes généraux de la protection des données (principes de la licéité, de la proportionnalité, de la finalité, etc.) doivent être respectés.

Indépendamment du fait qu'une base légale spéciale pour l'entraide administrative existe ou non, l'article 6 LPD doit, lors de l'entraide administrative, être respecté comme suit: La LPD stipule que des données personnelles ne peuvent pas être communiquées à l'étranger si ceci peut constituer une atteinte grave à la personnalité des personnes concernées, notamment parce qu'une protection des données équivalente à celle de la Suisse fait défaut dans les pays destinataires. En d'autres mots, le maître de fichier doit vérifier si les principes énoncés dans la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) et dans le protocole additionnel de cette convention concernant les autorités de surveillance et la transmission de données transfrontière sont respectés. Le maître de fichier doit d'autre part également s'assurer que les principes fondamentaux de la LPD sont respectés (à savoir que la personne concernée peut défendre ses intérêts au cas où ces principes ne sont pas respectés, que le droit d'accès est garanti et qu'il existe un organe de surveillance indépendant). L'examen d'adéquation mentionné ci-dessus peut également être effectué sur la base de la liste (non exhaustive) des Etats publiée sur notre site web. Au cas où les données sont communiquées dans un pays qui, selon cette liste, dispose d'un niveau de protection des données adéquat, l'article 6 LPD est en principe considéré comme étant respecté (sauf bien sûr dans les cas où il existe des indices concrets de violation de la protection des données). Il y a lieu en outre de tenir compte du fait que dans certains États la législation sur la protection des données n'est – contrairement à la Suisse – pas applicable aux personnes morales, ce qui signifie que l'article 6 LPD ne serait pas non plus respecté dans les cas où les données communiquées concernent des personnes morales.

Lorsqu'une législation adéquate sur la protection des données fait défaut, des garanties suffisantes doivent être données d'une autre manière. Dans le cadre d'une entraide administrative transfrontière, ces garanties peuvent être fixées dans une clause de protection des données intégrée dans un accord ou éventuellement dans une déclaration séparée. En cas de communication de données personnelles sensibles, le traité international doit être ratifié par l'Assemblée fédérale (base légale au sens formel). La clause de protection des données doit être adaptée de cas en cas au domaine concerné et contenir certains points précis. Les clauses contractuelles standards de l'UE ainsi que le contrat modèle du Conseil de l'Europe se trouvent à titre d'exemple sur notre site web.

Dans les cas où il n'existe ni législation sur la protection des données adéquate ni clause de protection des données, on peut en dernier ressort vérifier s'il n'existe pas une autre exception prévue par la loi. Ces exceptions doivent néanmoins être appliquées de manière très restrictive.

1.2.11 Protection des données et RFID

La plupart des citoyens connaissent la technologie RFID (Radio Frequency Identification) par les commerces, dans lesquels des appareils de lecture et écriture sont placés près de la caisse. Lorsqu'une radio-étiquette RFID non désactivée se trouve encore sur ou dans un produit, le lecteur déclenche une alarme au passage. De telles étiquettes se rencontrent de plus en plus fréquemment sur les marchandises, mais se trouvent également p.ex. dans les titres de transport des chemins de fer de montagne, les livres de bibliothèque, les dispositifs antidémarrage de voitures et la gestion des bagages d'avions. La technologie RFID présente en particulier le risque de pouvoir traiter des données à l'insu des personnes intéressées.

Nous avons traité le sujet «Protection des données et RFID» lors d'une conférence à l'EPF de Zurich. Au début de la décennie, il a été de plus en plus souvent question de cette nouvelle technologie. Nous n'étions alors pas sûrs dans quelle mesure celle-ci serait couverte par la LPD et avions donc décidés de l'analyser. Cette analyse a permis de tirer les conclusions suivantes: la technologie RFID n'est pas aussi récente que ne le laissaient supposer les premières informations. Elle a été mise en œuvre à la fin de la deuxième guerre mondiale déjà pour l'identification ami/ennemi. Du point de vue organisationnel, la RFID peut être considérée comme une «nouvelle» ressource aux propriétés spéciales dans un système, p. ex. une application. Cette ressource présente des caractéristiques particulières qui peuvent porter préjudice à la protection des données.

Un risque fondamental réside dans le fait que les données dans un transpondeur ou «tag» (étiquette RFID) peuvent être traitées jusqu'à une certaine distance par des ondes radio. A cet effet, aucun contact visuel direct n'est nécessaire, pas plus qu'une intervention active de la personne concernée. En d'autres termes, cela signifie que le traitement des données peut avoir lieu à l'insu de la personne concernée. Toutes les données qui sont enregistrées sur des puces RFID et qui ne sont pas détruites, effacées ou spécialement protégées peuvent être manipulées par des appareils de lecture et écriture (cachés). Si celles-ci sont interconnectées avec des données provenant d'autres sources, le risque existe que des profils d'achat ou de déplacement

puissent être établis. Les étiquettes RFID sont souvent liées en un système constitué de réseaux, de stations de travail, de serveurs et autres éléments, de manière que l'élaboration d'une application RFID conforme à la protection des données (de la collecte des données jusqu'à leur anonymisation ou leur effacement) doit également les prendre en compte. Il s'agit donc d'inclure au système à construire les dispositions suivantes importantes en matière de protection des données:

- Transparence: L'utilisation de la technologie RFID doit être reconnaissable pour la personne concernée. Celle-ci peut faire valoir son droit d'accès auprès du maître d'un fichier. Quiconque fait valoir un intérêt légitime peut exiger du maître de fichier que celui-ci corrige les données, en interdise la communication à des tiers ou y apporte une mention. Le maître du fichier doit documenter le système de manière appropriée. Cette documentation sera d'autant plus détaillée que les données personnelles traitées ou le but du traitement de données sont sensibles. A défaut, outre le manque de gouvernabilité de tels systèmes, le principe de transparence n'est pas respecté.
- Finalité: les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.
- Proportionnalité: les systèmes doivent être conçus de manière que le minimum de données personnelles soient nécessaires pour l'accomplissement des tâches. On utilisera autant que possible des données anonymisées; en l'absence de rapport avec une personne, la loi LPD n'est plus applicable. Dans la mesure où une identification des personnes est requise, les systèmes seront conçus pour permettre de travailler avec des pseudonymes. Par ailleurs, il faut effacer toutes les données qui ne sont plus nécessaires au but du traitement de données.
- Licéité: le traitement des données ne doit violer aucune législation, donc ni la loi LPD, ni d'autres lois ou ordonnances. Les personnes privées peuvent traiter des données personnelles si elles ont un motif justificatif. Il peut s'agir d'une base légale, du consentement de la personne concernée ou d'un intérêt prépondérant public ou privé.
- Consentement: dans la mesure où le consentement de la personne concernée est requis pour le traitement de données personnelles, celui-ci n'est valable que s'il intervient librement, sur la base d'informations appropriées. Cela signifie notamment qu'il faut communiquer à la personne concernée quelles données sont traitées où et comment, et quand elles seront effacées. Par ailleurs, lors du traitement de données personnelles sensibles ou de profils de la

personnalité, le consentement doit être explicite. Celui-ci doit être donné par la personne concernée sous forme écrite ou orale. Du fait de qu'un consentement oral est souvent difficile à prouver, nous recommandons en principe de requérir un consentement explicite par écrit. Par ailleurs, la personne concernée a le droit de révoquer en tout temps son consentement pour le traitement de données.

- Sécurité des données: les données personnelles doivent être protégées en particulier contre les traitements de données non autorisés et des erreurs techniques par des mesures techniques et organisationnelles appropriées. Les systèmes qui traitent des données personnelles sensibles ou des profils de la personnalité, ou servent à des buts sensibles, doivent notamment être protégés conformément à l'état actuel de la technique. Il faut également veiller à assurer la confidentialité, la disponibilité et l'intégrité des données.
- Contrôle: Les contrôles donnent confiance. Ces contrôles peuvent être effectués aussi bien par des collaborateurs internes que par des mandataires externes. Afin d'améliorer la protection des données ainsi que la sécurité des données ou de l'information, des organes accrédités pourront à l'avenir évaluer et certifier les différents systèmes.

1.2.12 Protection de données sensibles sur des systèmes de stockage

Les procédés de chiffrement sont des mesures appropriées pour protéger des données sensibles sur des systèmes de stockage tels que les disques durs et clés USB. Il faut considérer toutefois que les systèmes d'exploitation ou les applications enregistrent aussi les données sensibles (ou une partie d'entre elles) dans d'autres fichiers tels que des fichiers d'échange et des fichiers temporaires. Ces derniers doivent également être protégés. L'accès à des données chiffrées ne s'effectue la plupart du temps que par l'intermédiaire d'un mot de passe, raison pour laquelle celui-ci doit être sûr. Plusieurs outils de chiffrement sont disponibles aujourd'hui sur le marché. Non avons examiné les deux programmes Rohos Mini Drive et TrueCrypt quant à leur applicabilité.

Les données sensibles sur les systèmes de stockage électronique devraient être chiffrées. Par exemple, en cas de perte ou d'oubli d'un ordinateur portable éteint ou verrouillé, il devient ainsi difficile voire impossible pour une personne non autorisée de déchiffrer les données. Ceci s'applique également aux clés de stockage USB perdues.

Les outils de chiffrement disponibles aujourd'hui en partie gratuitement pour un usage personnel et téléchargeables depuis Internet utilisent des algorithmes de chiffrement tels que notamment AES256, qui correspond à l'état actuel de la technique. Cet algorithme ainsi que de nombreux autres ont été publiés, de sorte que leur sécurité a aussi pu être contrôlée par des services indépendants. Dans les systèmes de chiffrement, il faut toutefois considérer l'ensemble du procédé, du chiffrement des données initialement disponibles sous forme de texte en clair, jusqu'à leur déchiffrement (mise en œuvre globale des mesures de sécurité dans le système). Par ailleurs, il s'agit de relever que les systèmes d'exploitation et les applications enregistrent des données p. ex. dans des fichiers d'échange de type swapfile ou pagefile.sys, qui peuvent être lus par un agresseur potentiel en cas de protection insuffisante. En l'état actuel de nos connaissances, il existe les possibilités suivantes pour «sécuriser» ces fichiers d'échange:

- on efface ce fichier, puis on s'assure que la mémoire vive (RAM) est suffisamment grande pour qu'un échange (swapping) ne soit plus nécessaire; ou
- on efface physiquement le contenu du fichier d'échange au moment d'arrêter l'ordinateur.

Il est en outre important de chiffrer le cache des fichiers hors ligne (base de données hors ligne); à défaut, toutes les données du réseau stockées temporairement sur l'ordinateur s'y trouveraient sous forme non codée. Sur la base des applications utilisées, l'ordinateur crée encore d'autres fichiers, qui peuvent le cas échéant contenir des données sensibles, à l'exemple des fichiers (Internet) temporaires. Il convient d'effacer les fichiers temporaires à l'aide d'un outil approprié si l'on se trouve p.ex. dans un café Internet. Il y serait aussi facile d'installer des enregistreurs de frappes (keyloggers) permettant d'espionner les mots de passe sans que l'utilisateur ne le remarque. Sur son propre ordinateur, il est conseillé de faire effacer de manière automatique les informations sensibles à l'arrêt de l'ordinateur, de façon qu'au redémarrage il n'existe plus de données «anciennes». Une autre solution possible consiste à chiffrer l'ensemble de la partition système, de manière que p.ex. tous les fichiers d'échange ou temporaires soient enregistrés sous forme codée, inaccessible à des personnes non autorisées. L'ordinateur est ainsi plus fortement sollicité, par contre il n'y a plus lieu d'effacer les différents fichiers (temporaires).

Dans la plupart des cas, l'accès aux données chiffrées ou à l'outil de chiffrement s'effectue à l'aide d'un mot de passe. Celui-ci doit être constitué de sorte à ne pouvoir être que difficilement cassé. Il sera aussi long et complexe que possible et comportera donc au moins huit caractères, comprenant des minuscules, des majuscules, des chif-

fres et des caractères spéciaux. On peut composer un tel mot de passe en écrivant par exemple une phrase et en utilisant la première lettre de chaque mot, ainsi que des chiffres et signes de ponctuation (par exemple Qsl3pl+aeS? pour «Quelles sont les trois pommes les plus appréciées en Suisse?»). Les mots de passe en clair ne doivent pas être conservés dans des lieux non sûrs. En guise de protection supplémentaire, on peut, outre le mot de passe (savoir), utiliser aussi une carte à puce ou une clé USB (possession), voire une donnée biométrique (caractéristique propre à une personne telle que l'empreinte digitale). Ceci permet d'accroître la sécurité des données.

A titre d'exemples, nous avons analysé les deux programmes de chiffrement Rohos Mini Drive et TrueCrypt quant à leur applicabilité. Rohos Mini Drive s'utilise sur des clés de stockage USB. TrueCrypt permet de traiter des données sous forme chiffrée notamment sur des disques durs et, avec les droits d'administrateur, aussi sur des clés de stockage USB.

Rohos Mini Drive, version 1.6.0.0, requiert la configuration minimale suivante: Windows 2000/XP/2003/Vista; connexion USB 1.1/2.0; clé USB à mémoire flash ou U3 Smart Flash Drive avec 1 Mb ou plus d'espace mémoire; la taille maximale de la partition chiffrée est de 2 Gb. Le programme de chiffrement Rohos Mini Drive peut servir au chiffrement de données sur des clés de stockage USB. Dès que le programme est installé sur une telle clé, il est ensuite utilisable sur n'importe quel ordinateur sans droits d'administrateur. Le déchiffrement est effectué par décodage du document dans un dossier «caché» et ouverture dans l'application appropriée. Le dossier et les documents traités (déchiffrés) qui s'y trouvent restent en place lorsque l'on quitte Rohos Disk Browser. Il est donc important d'effacer ces fichiers temporaires afin que ceux-ci ne puissent pas être lus par d'autres personnes. Lors de notre essai, nous avons effacé les fichiers temporaires et constaté que cet effacement s'effectue de manière logique et non physique. A l'aide d'outils de récupération, nous sommes parvenus à restaurer les fichiers. L'utilisateur doit donc être conscient du fait qu'il doit encore les effacer avec un outil de nettoyage (wipe tool) séparé pour qu'ils ne puissent plus être reconstitués.

Rohos laisse espérer une nouvelle version qui permettra de procéder au déchiffrement directement dans les applications concernées, de manière qu'il n'y ait plus de fichiers temporaires enregistrés sur le disque.

TrueCrypt (version 6.2.a) est un logiciel libre (open source) pour le chiffrement de supports de données. Il est utilisable sur les systèmes d'exploitation suivants: Windows 2000, XP, 2003, Vista, 7; Linux, Mac OS X, Mac OS X/Intel.

Les utilisateurs qui ne disposent pas des droits d'administrateur ont la possibilité d'utiliser TrueCrypt sous une forme comportant quelques restrictions. Ils peuvent notamment créer des volumes (FAT), mais pas des partitions, dans lesquels les fichiers sensibles seront traités en toute sécurité par des procédés de chiffrement. Par ailleurs, il n'est pas non plus possible de créer des volumes NTFS et d'utiliser TrueCrypt en mode «portable» ou «traveler». Le programme TrueCrypt Traveler Mode, qui peut par exemple être installé sur une clé de stockage USB, n'est utilisable que sur des systèmes pour lesquels on dispose des droits d'administrateur.

Le chiffrement et déchiffrement s'effectuent à la volée (on-the-fly), c'est-à-dire en temps réel (real-time encryption). Dans ce procédé, le chiffrement et déchiffrement s'effectuent «directement» en mémoire vive (RAM), sans création de fichiers temporaires. Pour procéder à ce chiffrement en temps réel, TrueCrypt nécessite des pilotes (device drivers). Les utilisateurs qui ne disposent pas des droits d'administrateur ne peuvent ni installer, ni lancer de pilotes sous Windows.

1.3 Internet et télécommunication

1.3.1 La cyberadministration et le citoyen numérique

Le nouveau numéro AVS est de plus en plus utilisé comme identificateur de personne dans divers projets de cyberadministration. On ignore volontiers dans ce contexte qu'une utilisation de ce numéro à ces fins doit d'abord faire l'objet d'une base légale.

Les projets de cyberadministration de la Confédération avancent à grands pas. Dans ce cadre, nous constatons que les personnes impliquées dans ces projets ne nous contactent souvent qu'en passant, et très tard, à propos des problèmes liés à la protection des données.

Un problème général qui se pose dans le domaine de la cyberadministration est celui de l'authentification des citoyens. Comment l'État peut-il par exemple constater que le citoyen X ayant droit de vote a déposé son vote par voie électronique ou que c'est réellement la citoyenne Y qui a communiqué par voie électronique son départ à sa commune?

Pour beaucoup de personnes, la solution la plus simple consisterait à utiliser le nouveau numéro d'assuré à 13 chiffres comme authentification numérique. Dans des rapports d'activités précédents, nous avons cependant déjà insisté sur le fait qu'une utilisation à large échelle du numéro AVS comme identificateur de personne présentait de gros risques pour les citoyens, parce qu'elle permettrait d'établir des connexions que ceux-ci ne peuvent pas prévoir. Pour qu'une utilisation générale du numéro AVS comme identificateur de personne soit au moins légitimée par la volonté populaire et que le débat politique nécessaire ait lieu, celle-ci doit être réglementée de manière suffisante au niveau législatif. C'est là une condition que l'on oublie facilement lors de la planification des divers projets et que l'on prend insuffisamment en compte dans les calendriers de réalisation.

Nous avons une nouvelle fois mentionné ces points dans notre prise de position sur la norme e-CH 0045, qui comprend un glossaire pour le domaine du registre électoral.

1.3.2 Prises de vue des voies publiques sur Internet: Google Street View

Après examen approfondi de Google Street View, nous avons estimé que ce service de navigation en ligne présentait des lacunes importantes du point de vue de la protection des données. Par ailleurs, nous avons reçu de nombreuses plaintes de personnes concernées. Nous avons donc établi une recommandation, puis déposé plainte contre Google auprès du Tribunal administratif fédéral.

Depuis la mise en ligne du service Google Street View à la mi-août 2009, tant le PFPDT que Google Switzerland GmbH ont reçu de nombreuses protestations émanant de la population à propos de l'insuffisance ou l'absence de floutage des visages et des plaques d'immatriculation des véhicules. Nos recherches ont confirmé ces constatations. Nous avons en outre constaté que les informations données par Google sur les trajets empruntés par la caméra étaient lacunaires et géographiquement imprécises. Nous avons informé Google de ces constats et les responsables de l'entreprise ont proposé des mesures d'amélioration qui ne se sont cependant pas avérées convaincantes. Nous maintenons qu'une anonymisation complète des visages et des plaques d'immatriculation des véhicules est nécessaire pour garantir le respect de la sphère privée. Nous avons donc exigé dans notre recommandation du 11 septembre 2009 que Google:

- développe une meilleure solution afin que les visages et les plaques d'immatriculation ne puissent plus du tout être reconnus,
- apporte une attention particulière à l'anonymisation des installations sensibles telles que les hôpitaux, les écoles ou les prisons,
- efface les images de rues privées prises en l'absence de consentement,
- élimine les images de lieux fermés (cours, jardins) et diminue à l'avenir la hauteur de montage des caméras,
- informe une semaine avant d'effectuer les prises de vue et une semaine avant leur mise en ligne quels sont les villes et villages concernés,
- ne publie pas de nouvelles images prises en Suisse jusqu'à ce que les questions juridiques soient clarifiées.

Google a rejeté la plupart des mesures recommandées. Nous avons donc porté plainte devant le Tribunal administratif fédéral contre Google, Inc. et contre Google Switzerland GmbH et demandé, à titre de mesure provisionnelle, qu'aucune image prise en Suisse ne soit mise en ligne et qu'aucune nouvelle prise de vue n'y soit autorisée. Nous avons convenu d'un accord avec Google en décembre de la même année. Cet accord répond entièrement aux buts recherchés par les mesures provisionnelles: pendant la durée de la procédure judiciaire, Google ne mettra en ligne aucune nouvelle image prise en Suisse. Lors de prises de vue sur la voie publique, les personnes potentiellement concernées seront informées en temps voulu. Google s'engage en outre à se soumettre au jugement exécutoire que rendra la justice suisse dans cette affaire et à l'appliquer à toutes les prises de vue réalisées en Suisse et déjà conservées à l'étranger. Cet accord a été examiné et approuvé par le Tribunal administratif fédéral.

La recommandation et le mémoire de demande sont reproduites, en version allemande, à l'annexe 4.1.6 / 4.1.7. Ces documents peuvent en outre être consultées sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des données – Recommandations/ Actions en justice.

1.3.3 Prises de vue de la voie publique sur Internet: Touchtown

Une entreprise exploite sur le site «touchtown.ch» un produit concurrent à Google Street View, aux fonctions tout à fait comparables. Toutefois, par rapport à Google, la société Annularspace GmbH a une autre approche de la collecte de données que nous considérons comme conforme aux principes de la protection des données.

Bien que dans certains cas, les personnes concernées soient aisément reconnaissables et que les visages n'aient pas été floutés, nous n'avons pas qualifié le service «Touchdown» de contraire à la protection des données, ceci sur la base de nos analyses. Contrairement à Google, Inc., la société Annularspace GmbH fait ses prises de vue avec des appareils enregistreurs portables et informe les personnes concernées avant la prise de vue à l'aide de haut-parleurs et de tracts. De cette manière, les personnes concernées ont la possibilité de s'éloigner de l'angle de prise de vue de la caméra pour ne pas être photographiées. Dans les cas où la foule ou les circonstances locales ne le permettent pas, les personnes photographiées sont, selon les indications de l'entreprise, manuellement rendues méconnaissables. En outre, à ce jour, nous n'avons pas eu connaissance de prises de vue de la sphère privée sans que le consentement des personnes concernées n'ait été requis auparavant. Nous n'avons en tout cas reçu aucune réclamation de personnes éventuellement concernées.

1.3.4 Analyse de l'utilisation de sites web

Google Analytics est un service d'analyse de l'utilisation de sites web fourni par la société Google, Inc. Les données nécessaires sont transmises aux serveurs de Google situés aux Etats-Unis pour y être analysés. La société Google ayant adhéré aux principes de la «sphère de sécurité» (Safe harbor), Google Analytics peut être utilisé à certaines conditions tant par les organes fédéraux que par des particuliers sans que des garanties spécifiques ne doivent être convenues.

Le service Google Analytics fournit aux exploitants de pages Internet des données statistiques sur les accès à leur site sans qu'il ne soit nécessaire d'installer ou d'exploiter des programmes supplémentaires du côté du serveur; il leur permet également d'analyser ces données. Pour ce faire, les exploitants doivent intégrer à leur site web un code de programme fourni par la société Google, grâce auquel cette dernière saisit les accès au site, transmet ces données aux Etats-Unis et les traite pour les fournir ensuite à l'exploitant. Ces opérations constituent une communication de données à des tiers (dans ce cas Google) dans le cadre d'une relation d'externalisation; l'exploitant qui utilise Google Analytics doit donc informer les utilisateurs de son site dans une décharge de responsabilité que leurs données seront traitées par Google, Inc. aux Etats-Unis. Google met à disposition une telle décharge. Il incombe donc aux exploitants d'informer de manière complète les utilisateurs de leur site web du recours à Google Analytics.

1.3.5 Télévision par Internet

Nous avons examiné les prestations de services d'un fournisseur de télévision par Internet établi en Suisse sous l'angle de leur compatibilité avec la loi sur la protection des données et les avons approuvées. Nous avons procédé à cet examen sur la base de nos «Explications concernant la télévision numérique, la télévision interactive et la télévision par Internet».

La télévision par Internet rencontre un succès grandissant. Comme nous l'avons retenu dans nos «Explications concernant la télévision numérique, la télévision interactive et la télévision par Internet», ce phénomène va néanmoins de pair avec la possibilité d'enregistrer le comportement télévisuel des utilisateurs. Nous avons profité de l'occasion pour prendre contact avec les grands fournisseurs de télévision numérique et avec un fournisseur de télévision sur Internet, afin d'examiner quelles données personnelles ils traitaient et dans quel but. Dans tous les cas, nous avons constaté

que le traitement des données avait lieu en conformité avec la LPD. En particulier le fournisseur du service de télévision par Internet se distingue par une collecte limitée de données personnelles et par des délais de conservation dont la durée est inférieure à la moyenne.

Les explications mentionnées se trouvent sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Autres thèmes.

1.3.6 Explications concernant le traitement mobile de données

L'homme moderne est mobile et aimerait pouvoir travailler et avoir accès à ses documents n'importe où, que ce soit à la maison, au bureau ou en déplacement. Il existe plusieurs moyens de permettre cela. Par exemple, la personne peut emporter ses données sur un support ou les déposer quelque part sur Internet. Chaque solution présente certains risques qui peuvent être contrés par des mesures adéquates. Dans ce feuillet, nous distinguons quatre scénarios généraux et présentons pour chacun d'eux non seulement les avantages et inconvénients, mais aussi les risques en matière de protection des données. Finalement, nous montrons comment ces risques peuvent être contrés. Les explications sur le traitement mobile des données sont publiées dans l'annexe 4.1.1 ou sur notre site web www.leprepose.ch sous la rubrique Thèmes – Protection des données – Internet.

1.3.7 Explications concernant l'utilisation des moteurs de recherche

Sans moteurs de recherche, il serait quasiment impossible de s'y retrouver sur Internet, avec ses milliards de pages. Pour faciliter sans cesse la recherche d'informations sur la Toile, les moteurs de recherche doivent toutefois recenser de manière ciblée les informations sur le comportement de recherche des internautes et sur la qualité des résultats, mais aussi les évaluer selon des méthodes statistiques. Ce faisant, ils s'immiscent dans la sphère privée des internautes en traitant des données les concernant, tant lors de l'évaluation des requêtes que lors de la fourniture des résultats des recherches. Des informations et des conseils à ce sujet se trouvent dans notre document «Informations et conseils concernant l'utilisation des moteurs de recherche», publié dans l'annexe 4.1.2 ou sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet.

1.3.8 Introduction de la messagerie sécurisée (secure messaging)

Le PFPDT est récemment passé de PGP à la solution officielle de messagerie sécurisée. Les actuels certificats de classe C présentent par rapport à ceux de la classe B, réputés plus sûrs, des inconvénients, tels que l'absence de contrôle par l'utilisateur et l'accessibilité des clés privées sans mot de passe, mais aussi des avantages quant à la simplicité d'utilisation et à la sécurité cryptographique.

Depuis le 1er janvier 2000, nous avons bénéficié d'une solution non officielle de messagerie électronique sécurisée, chaque poste de travail disposant du logiciel PGP (Pretty Good Privacy). Nous avons ainsi été en mesure d'échanger des messages chiffrés et/ou signés avec l'ensemble des membres de la communauté mondiale PGP, qui représente une forme simplifiée d'infrastructure à clés publiques (PKI).

Cette page est désormais tournée avec l'introduction de la solution officielle «Secure Messaging» dans notre service. Chaque collaborateur dispose désormais d'un certificat électronique de classe C pour la signature et le chiffrement des courriels. Cette dernière opération n'est possible qu'avec des destinataires (internes ou externes) bénéficiant également d'une messagerie sécurisée de type S/MIME. Les certificats de classe C favorisent clairement la simplicité d'utilisation, étant donné qu'ils sont conservés dans le profil de l'utilisateur et qu'ils ne requièrent aucun mot de passe pour la signature par l'expéditeur ou le déchiffrement par le destinataire du message. La situation est différente avec des certificats de classe B (ou A), puisque ceux-ci sont stockés sur une carte à puce individuelle et exigent un mot de passe pour chaque signature ou déchiffrement d'un message. On peut ici relever que les certificats de classe B sont à cet égard plus sûrs que ceux de la classe C, mais que ces derniers sont cryptographiquement plus sûrs avec des clés RSA d'une longueur double, soit de 2048 bits. Rappelons qu'un nombre entier RSA de 768 bits (232 chiffres décimaux) vient d'être factorisé à l'aide de «moyens raisonnables», ce qui confirme le pronostic selon lequel les clés RSA de 1024 bits (dont les certificats de classe B) ne sont sûres plus que pendant quelques années encore.

1.4 Justice/Police/Sécurité

1.4.1 Mise en œuvre Schengen: Contrôle du PFPDT auprès de la représentation diplomatique suisse au Caire

En tant qu'autorité de surveillance des organes fédéraux en matière de protection des données, nous sommes chargés de contrôler les traitements de données personnelles du système d'information Schengen. Dans ce contexte, nous avons procédé à un contrôle auprès de la représentation diplomatique suisse en Egypte. Sur la base de nos constatations, nous avons rendu nos conclusions et adressé des propositions d'amélioration au Département fédéral des affaires étrangères (DFAE).

En tant qu'autorité de surveillance, nous contrôlons les traitements de données personnelles effectués par les organes fédéraux autorisés à utiliser le Système d'information Schengen (SIS), ce conformément aux exigences requises par la coopération Schengen. Nous effectuons, entre autres, ces contrôles auprès des représentations diplomatiques et consulaires suisses à l'étranger.

Dans ce contexte, nous avons procédé à un contrôle auprès de la représentation diplomatique suisse au Caire, en Egypte. Sur la base de nos constatations, nous avons rendu nos conclusions dans un rapport et adressé des propositions d'amélioration que le DFAE a acceptées et mises en œuvre. Le DFAE a notamment défini les responsabilités et les tâches des personnes chargées de la sécurité et de la protection des données dans les représentations suisses à l'étranger dans une directive interne. Il a également modifié la pratique de gestion des mots de passe conformément aux directives concernant la sécurité informatique dans l'administration fédérale. Il a limité l'accès aux salles des serveurs du réseau informatique de la représentation suisse au Caire aux seules personnes autorisées (responsables du service informatiques). Il a instauré des règles précises concernant la sauvegarde des données personnelles traitées par la représentation suisse. De plus, le DFAE poursuit ses activités d'instruction et de sensibilisation de ses collaborateurs en matière de protection des données.

L'absence de dispositif de communication sécurisé pour la communication de données par courriels entre les représentations suisses à l'étranger et les autres services de l'administration fédérale demeure cependant problématique. Ce problème souligné par le préposé fédéral est actuellement traité par l'Office fédéral de l'informatique et de la télécommunication (OFIT) qui met en place des mesures de sécurité et de protection des données en la matière pour les offices fédéraux.

D'autres textes sur Schengen se trouvent dans ce chapitre ainsi qu'au chiffre 1.10.1.

1.4.2 Mise en œuvre Schengen: Logfiles SIS

Les accès à la partie nationale du système d'information Schengen (N-SIS) sont enregistrés dans des fichiers de journalisation (logfiles). Pour accomplir leurs tâches, les autorités de protection des données doivent les analyser. Nous avons, en collaboration avec l'office fédéral de la police, examiné la structure des logfiles de N-SIS et leur utilisation.

Selon les accords de Schengen, la Suisse dispose d'une copie nationale de la base de données SIS (N-SIS). Les informations contenues dans le N-SIS sont des données sensibles et seul un groupe restreint de personnes y a accès. Tous les accès à la base de données N-SIS sont enregistrés dans des fichiers journaux (logfiles). Ceux-ci permettent de savoir qui a fait quoi, quand et pourquoi. Dans le cadre des leurs compétences respectives, les autorités de protection de données nationale et cantonales doivent pouvoir analyser les logfiles de leurs utilisateurs finaux.

En collaboration avec l'Office fédéral de la police (fedpol), nous avons eu la possibilité d'examiner la structure des logfiles du N-SIS. De cette façon, il nous sera possible de mieux cibler nos requêtes de voir des extraits des logfiles et d'aider plus efficacement les cantons dans leurs requêtes. Nous avons présenté ces éclaircissements au groupe de coordination Schengen des autorités de protection des données lors de notre réunion du 12 novembre 2009 et expliqué à nos collègues cantonaux la procédure d'utilisation des fichiers de journalisation.

D'autres textes sur Schengen se trouvent dans ce chapitre ainsi qu'au chiffre 1.10.1.

1.4.3 Mise en œuvre Schengen: contrôle du PFPDT auprès de la Police judiciaire fédérale

Le premier contrôle relatif aux traitements des données effectués dans le Système d'information Schengen a montré que la Police judiciaire fédérale, en tant qu'utilisatrice finale, respecte les exigences légales de sécurité et de protection des données.

En raison de l'importance et de l'ampleur des traitements de données personnelles effectués dans le Système d'information Schengen (SIS) en Suisse depuis juin 2008, nous avons prévu de mener en 2009 un premier contrôle des traitements de données effectués dans le SIS et de l'utilisation de celui-ci. Nous avons ainsi décidé de vérifier la licéité de l'accès des collaborateurs de la Police judiciaire fédéral (PJF) ayant un droit d'accès au SIS (utilisateurs individuels) ainsi que le respect des exigences légales de sécurité et de protection des données lors de l'utilisation du SIS par ces mêmes colla-

borateurs. Quelques autorités de protection des données cantonales ont également procédé à des contrôles auprès d'utilisateurs cantonaux du SIS.

Nous avons demandé à l'Office fédéral de la police (fedpol) de nous fournir les différentes documentations relatives aux traitements des données du SIS. Nous avons procédé à une analyse de la documentation reçue afin d'affiner notre questionnaire utilisé lors du contrôle sur place. Ce contrôle a eu lieu en juin 2009 et a porté sur différents points. Il nous a permis de voir de quelle manière les collaborateurs de la PJF ont accès aux données du SIS et quelles procédures ont été mises en place en cas de traitement illicite ou lorsqu'il apparaît que des données incorrectes figurent dans le SIS. Nous avons également vérifié les profils des collaborateurs de la PJF ayant un droit d'accès au SIS. Les mesures techniques et organisationnelles de sécurité ont également été analysées. Les locaux de la PJF sont sécurisés (loge à l'entrée du bâtiment et accès dans les différents locaux uniquement avec des badges individuels). L'accès au SIS n'est possible qu'à partir d'un ordinateur avec une adresse IP autorisée en utilisant uniquement une carte cryptographique et le mot de passe correspondant. L'analyse des fichiers de journalisation n'a pas été effectuée lors de ce contrôle. Une telle analyse nécessitait des informations supplémentaires de la part de fedpol qui ont été fournies après l'exécution du contrôle. Nous avons pu ainsi fournir les informations utiles sur l'utilisation des fichiers de journalisation à l'autorité de protection des données du canton de Berne dans le cadre de ses propres activités de surveillance. Nos prochains contrôles auprès d'autres utilisateurs fédéraux porteront également sur l'analyse des fichiers de journalisation.

En conclusion, nous avons constaté lors de ce contrôle que la PJF, en tant qu'utilisatrice finale du SIS, respectait les exigences légales de sécurité et de protection des données. Nous n'avons ainsi pas eu à formuler de remarque ou de recommandation. D'autres textes sur Schengen se trouvent dans ce chapitre ainsi qu'au chiffre 1.10.1.

1.4.4 Groupe de coordination Schengen des autorités suisses de protection des données

Sur la base de l'ordonnance correspondante, nous avons pris l'initiative de constituer un groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre des accords d'association à Schengen. Nous avons convoqué ce groupe de coordination à deux reprises en 2009.

L'article 54 de l'ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau Sirene prévoit que les autorités cantonales de protection

des données et le PFPDT collaborent activement dans le cadre de leurs compétences respectives et exercent une surveillance coordonnée du traitement de données personnelles. Sur la base de cette disposition légale, nous avons pris l'initiative de constituer un groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre des accords d'association à Schengen (ci-après: groupe de coordination).

Le groupe de coordination est une plateforme permettant aux autorités cantonales et fédérale de protection des données de coopérer activement dans le cadre de leurs compétences de surveillance des traitements de données effectués en application des accords d'association à Schengen. Agissant dans le respect des compétences de chacun de ses membres, le groupe de coordination a notamment les tâches suivantes: échanger les informations nécessaires à la surveillance effective des traitements de données personnelles contenues dans les banques de données de l'espace Schengen; examiner les difficultés d'interprétation ou d'application des dispositions légales; étudier les problèmes pouvant se poser lors d'activités de surveillance ou dans l'exercice des droits des personnes concernées; formuler des propositions ou des avis harmonisés en vue de trouver des solutions communes; soutenir et coordonner les activités de surveillance de chacun de ses membres. Le groupe de coordination est composé d'un représentant de chaque autorité de protection des données cantonale ainsi que d'un représentant du PFPDT, qui en assure le secrétariat.

Au cours de l'année 2009, nous avons convoqué le groupe de coordination à deux reprises. Lors de la réunion du 3 avril 2009, les travaux se sont concentrés sur l'élaboration d'un règlement nécessaire au bon fonctionnement du groupe de coordination. Nous avons également présenté le cadre et les objectifs des contrôles à effectuer auprès d'utilisateurs finaux du SIS. Nous avons en particulier expliqué les démarches que nous allions entreprendre en vue de notre contrôle annoncé auprès de la police judiciaire fédérale. Nous avons aussi présenté les résultats de notre contrôle effectué auprès de la représentation diplomatique et consulaire suisse à Kiev (Ukraine).

Lors de la réunion du 12 novembre 2009, le groupe de coordination a adopté son règlement de fonctionnement. A cette occasion, nous avons transmis aux participants cantonaux des informations sur les travaux en cours au sein de l'autorité de contrôle commune Schengen, du groupe de travail justice et police de la conférence européenne des commissaires à la protection des données et du groupe de coordination Eurodac. Nous avons également expliqué les procédures relatives aux contrôles des logfiles du SIS auprès du maître de fichier fedpol. Enfin, nous avons présenté les résultats de nos contrôles effectués auprès de la police judiciaire fédérale et auprès de la représentation diplomatique et consulaire suisse au Caire (Egypte). Les autorités de protection des données des cantons de Berne et de Fribourg ont également fait

part de l'avancement de leurs contrôles respectifs auprès de leurs autorités de police cantonales. Enfin, un groupe de travail a été chargé de mettre à disposition de tous les membres du groupe de coordination un document de méthodologie pour les activités de surveillance; ce document s'inspire de nos procédures de contrôle internes, des recommandations et meilleures pratiques de protection des données du catalogue Schengen adopté par le Conseil européen ainsi que du catalogue de protection des données visant à développer des standards de contrôle communs, élaboré par le groupe de travail justice et police de la conférence européenne des commissaires à la protection des données.

D'autres textes sur Schengen se trouvent dans ce chapitre ainsi qu'au chiffre 1.10.1.

1.4.5 Demandes d'accès concernant le système d'information ISIS

En 2009, le nombre des demandes d'accès concernant le système d'information ISIS n'a pas été aussi important qu'en 2008. Dans le cadre de la prochaine révision de la législation sur la sûreté intérieure et extérieure qui aura lieu en 2010, il est prévu d'introduire un droit d'accès direct comparable à celui applicable aux fichiers JANUS et GEWA.

En 2008, 148 demandes d'accès appelées indirectes concernant le système d'information ISIS avaient été déposées auprès de notre secrétariat (cf. notre 16e rapport d'activités 2008/2009, ch. 1.4.4). Nous avons reçu 34 demandes d'accès en 2009. Ce nombre de demandes équivaut au double des demandes déposées les années antérieures (1998 à 2007). Le Service de renseignement de la Confédération nous a indiqué que dans le cadre de la prochaine révision de la législation sur la sûreté intérieure et extérieure qui aura lieu en 2010, il est prévu de remplacer le système du droit d'accès dit indirect par un droit d'accès direct basé sur la législation régissant l'accès aux fichiers JANUS et GEWA (cf. notre 16e rapport d'activités 2008/2009, ch. 1.4.2 et notre 15e rapport d'activités 2007/2008, ch. 1.4.4).

1.4.6 Amélioration des prescriptions de sécurité pour les armes d'ordonnance

Les mesures adoptées dans le cadre de la détection de tout danger potentiel lié aux armes d'ordonnances nécessitent une attention particulière quant au traitement de données personnelles sensibles. Le principe de proportionnalité doit en particulier être respecté, notamment lors du recours à un contrôle de sécurité sans le consentement de la personne concernée.

Afin de déceler suffisamment tôt tout danger potentiel que peut présenter un détenteur d'armes d'ordonnance, le Conseil fédéral a proposé d'introduire de nouvelles mesures dans la législation militaire. Deux mesures touchent de manière importante la personnalité et les droits fondamentaux des personnes concernées. La première mesure implique le traitement, en particulier la communication de données sensibles relatives à la santé. Il s'agit du devoir d'annoncer applicable aux autorités fédérales, cantonales et communales ainsi qu'aux médecins, psychiatres et psychologues, lorsqu'ils ont connaissance de signes qu'un militaire pourrait représenter, avec son arme, un danger pour lui-même ou pour des tiers ou s'il y a d'autres indications d'un usage abusif. Les règles de protection des données devront être scrupuleusement respectées, en particulier en cas d'annonces infondées. Conformément à nos tâches de surveillance et en collaboration, le cas échéant, avec les autorités cantonales de protection des données, nous procéderons à des contrôles auprès des autorités militaires en charge du traitement de ces annonces.

La seconde mesure consiste en l'introduction d'un contrôle de sécurité, certes limité, mais sans le consentement de la personne concernée. Dans le cadre de la consultation des offices, nous avons exprimé l'avis que les autres mesures paraissaient suffisantes pour déterminer la dangerosité d'une personne et que le recours à un contrôle de sécurité ne devait avoir lieu que si cela s'avérait vraiment nécessaire. De plus, nous avons clairement mentionné dans notre prise de position que le recours à un contrôle de sécurité, même partiel, ne serait pas conforme au principe de proportionnalité. Le Conseil fédéral et le Parlement n'ont pas tenu compte de notre avis. Le Parlement a toutefois supprimé le caractère obligatoire de l'annonce.

1.4.7 Avant-projet de révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

Dans le contexte de l'introduction du nouveau code de procédure pénale suisse et dans le cadre de la consultation des offices, nous avons apporté diverses remarques sur l'avant-projet de révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Nous avons en particulier critiqué le manque d'informations sur l'efficacité de l'installation des programmes informatiques sur des systèmes de traitement des informations à l'insu des personnes concernées. Nous avons aussi critiqué la notion très vague de fournisseur de services Internet, ainsi que l'application confuse des délais de conservation.

Une modification de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) doit être effectuée dans le cadre de l'introduction du

code de procédure pénale. Nous avons apporté plusieurs remarques à ce sujet dans le cadre de la consultation des offices sur l'avant-projet.

L'avant-projet était surtout imprécis sur un point: la définition du cercle des personnes auquel la loi s'applique. Nous avons demandé que cela soit précisé. Nos critiques ont aussi porté sur le fait que les données enregistrées auprès du service de surveillance ne devraient pas être effacées. Nous estimons qu'il faut absolument intégrer des délais légaux d'effacement.

En matière de recherche urgente de personnes, nous estimons que la formulation «les données relatives à des tiers peuvent être également consultées» est trop générale et qu'elle comporte un risque considérable d'abus. Pour cette raison, les circonstances et le but devraient être circonscrits de manière plus précise.

En ce qui concerne la surveillance de la correspondance par poste, le projet de loi définit l'obligation de donner des renseignements sur la personne avec qui la personne surveillée a ou a eu des contacts par courrier postal. En outre, les données relatives au trafic et à la facturation devraient être conservées au moins pendant douze mois. A notre avis, les fournisseurs de services postaux pourraient être tenus, du fait de cette formulation, de stocker les connexions postales sur douze mois. Nous avons critiqué ce stockage des données et demandé que des modifications soient effectuées en conséquence.

Nous sommes très sceptiques quant à l'introduction secrète de programmes informatiques dans des systèmes de traitement des informations. D'une part, l'efficacité de ces programmes n'est pas suffisamment démontrée, d'autre part, leur introduction secrète sur l'ordinateur d'une tierce personne constitue une atteinte grave à sa sphère privée.

Nos critiques ont également visé l'imprécision de la notion de «fournisseurs Internet». On pourrait également compter parmi eux l'exploitant d'un réseau privé WIFI. Nous rejetons l'extension de l'obligation de surveillance des réseaux privés WIFI (p. ex. d'un hôtel ou d'un restaurant). Pour cette raison, nous avons proposé de remplacer la notion de «fournisseur Internet» par celle plus précise de «fournisseur de services de télécommunication».

1.5 Santé

1.5.1 Révision de la loi sur les épidémies: maladies infectieuses

Avec l'ordonnance du Département fédéral de l'intérieur (DFI) sur la prévention de l'introduction de nouvelles maladies infectieuses émergentes se pose le problème de la création d'une base légale claire. Ceci s'impose d'autant plus que la situation n'est pas non plus claire en ce qui concerne la communication transfrontière de données personnelles.

La grippe porcine a également laissé des traces au niveau de la protection des données. Nous avons été impliqués très tôt dans la procédure de consultation des offices relative à la «modification de l'ordonnance du DFI sur la prévention de l'introduction de nouvelles maladies infectieuses émergentes». C'est surtout au niveau du trafic aérien, dans les aéroports domestiques, que s'est posée la question de savoir dans quelle mesure il était permis de communiquer des données personnelles au-delà des frontières. Nous avons pourtant vite reconnu la nécessité de mettre en vigueur aussi rapidement que possible les modifications de l'ordonnance. En même temps, nous avons demandé à l'Office fédéral de la santé publique (OFSP) s'il n'était pas opportun de profiter de la révision en cours de la loi sur les épidémies pour créer une base légale suffisante dans ce domaine sensible de la santé publique. La même demande nous a en même temps aussi été adressée par le trafic aérien.

Selon la loi fédérale sur la protection des données, les organes fédéraux ne sont autorisés à traiter des données personnelles sensibles et des profils de la personnalité que si ceci est explicitement prévu par une loi au sens formel. La loi sur les épidémies ne contient cependant aucune base légale concrète justifiant le traitement de données prévu par l'OFSP. Une exception n'existe que si des circonstances extraordinaires l'exigent; dans un tel cas, le Conseil fédéral peut prendre les mesures nécessaires pour le pays entier ou pour certaines régions du pays. En outre, la loi sur les épidémies part du principe que les mesures permettant de lutter contre les maladies transmissibles doivent être prises par les cantons. Étant donné que la situation en matière de protection des données dans le domaine de la communication transfrontière de données personnelles n'est pas claire et que les données concernées par l'ordonnance (questionnaire de santé) sont des données personnelles sensibles, nous sommes d'avis qu'il est nécessaire de créer une base légale claire. Nous suivrons avec attention l'évolution de cette question.

1.5.2 Cybersanté (eHealth): appréciation de l'architecture proposée

L'architecture proposée pour la cybersanté (eHealth) peut être qualifiée de conforme aux exigences de la protection des données. Nous nous sommes particulièrement engagés dans le groupe restreint du projet partiel «Normes et architecture» pour que les exigences fondamentales telles que le droit à l'autodétermination en matière d'information soient prises en compte dans la structure décentralisée et l'adéquation de l'architecture.

En août 2009, les premières recommandations concernant les normes et l'architecture du projet de cybersanté (eHealth) ont été approuvées. Elles avaient pour objectif de contribuer à ce que les services électroniques de santé se développent dans une direction coordonnée. Comme le demande le Conseil fédéral, une haute priorité doit être accordée à la protection des données (cf. notre 16e rapport d'activités 2008/2009, ch. 1.5.3). La question se pose aujourd'hui de savoir si cette exigence a été prise en compte dans le sous-projet «Normes et architecture» et – encore plus important – quel impact cette exigence a sur l'architecture eHealth.

La première réponse est positive. La sensibilité pour les questions de protection des données existe dans le sous-projet, ce qui ne va pas de soi pour un projet d'une telle envergure.

La réponse à la deuxième question se trouve dans le document «Recommandations projet partiel, normes et architecture» de l'organe de coordination Confédération – cantons (sur le site web www.e-health-suisse.ch, sous la rubrique Mise en œuvre – Recommandations – Normes et architecture»). Ce document présente les éléments essentiels de l'architecture ainsi que les principes de base et les lignes directrices sur lesquelles ces éléments se basent. Une importance particulière a été accordée au droit à l'autodétermination en matière d'information, aux structures décentralisées et à la finalité de l'architecture. Le groupe restreint du projet, auquel nous participons régulièrement, a conçu une architecture qui prend en compte ces principes fondamentaux.

Dans les prochaines étapes, nous participerons de manière active en particulier à la définition des rôles que le personnel traitant peut assumer au sein d'eHealth, ainsi que des procédés d'identification.

1.5.3 Exigences minimales relatives aux formulaires d'admission des hôpitaux

Toute personne admise dans un hôpital doit en règle générale remplir un formulaire d'admission. Il n'existe cependant aucune obligation de signer ce formulaire dans son intégralité. Toutes les questions du formulaire doivent satisfaire à certains critères, qui permettent au patient ou à la patiente d'en vérifier la licéité. Nous avons en particulier examiné deux points.

Lorsqu'une personne est admise dans un hôpital, elle doit en règle générale remplir un formulaire d'admission. Les données administratives, telles que le nom, le prénom et l'adresse d'une personne constituent des données personnelles au sens de la LPD. Les données relatives à la santé sont quant à elles considérées comme des données personnelles sensibles. Nous avons été sollicités à plusieurs reprises pour prendre position sur la légalité des diverses questions figurant sur ces formulaires. Les hôpitaux n'utilisant pas tous les mêmes formulaires, il est nécessaire des les examiner un à un. Ci-dessous nous examinons deux points en particulier.

Les formulaires d'entrée peuvent notamment poser la question de la participation à un projet de recherche ou à une étude. Les patients doivent savoir qu'une telle participation a toujours lieu sur une base volontaire. Le consentement, qui doit être donné par écrit, n'est valable que si le participant a été suffisamment informé au préalable sur l'objectif et la finalité du projet ainsi que sur les traitements de données qui en résultent. Dans la pratique, ceci est fait par la remise de notices d'information et par des entretiens d'information. Pour qu'un consentement soit valable, les personnes concernées doivent être en mesure d'en reconnaître la portée (étendue et finalité). Ce n'est que dans ces conditions qu'un consentement est considéré comme consentement éclairé. A cet égard, le respect du principe de transparence dans la formulation des clauses de consentement et des formulaires d'information est déterminant. La personne qui participe à une étude doit en outre être informée en détail sur le but et le déroulement de l'étude ainsi que sur tous les traitements de données et mesures de protection des données (transmission, stockage, destruction des données, protection contre l'accès par des tiers non autorisés, mesures de pseudonymisation et d'anonymisation éventuellement prévues, etc.). Le caractère facultatif du consentement et la possibilité de révoquer ce dernier en tout temps doivent toujours être expressément mentionnés. Si une personne révoque son consentement, elle doit pouvoir partir de l'idée que toutes les données la concernant seront détruites. Pour plus de sûreté, il

est recommandé de demander une confirmation que ces données ont bien été supprimées. Les participants peuvent bien entendu accepter que les données qui ont été traitées dans le cadre de l'étude jusqu'à la révocation continuent à être utilisées. Une clause à ce sujet devrait figurer dans la déclaration de consentement. Un tel consentement peut également être révoqué en tout temps en vertu du droit à l'autodétermination en matière d'information. Si l'utilisation subséquente des données n'est pas réglée, on ne peut sans autre partir du principe que les données peuvent continuer à être utilisées, sauf si elles ont été anonymisées. A partir du moment où tous les attributs permettant d'identifier une personne concernée ont été retirés, une utilisation subséquente n'est plus sujette au consentement du participant puisque l'on n'a dans ce cas plus affaire à des données personnelles.

Un deuxième point est l'externalisation: Il est aujourd'hui courant qu'un médecin ou un hôpital fasse appel à des organisations professionnelles extérieures pour l'exécution de certains travaux administratifs. Dans la mesure où de tels tiers ne reçoivent pas de données relatives aux patients (comme c'est p. ex. le cas pour des clôtures comptables), cela ne pose aucun problème du point de vue de la protection des données. Par contre, les services chargés d'imputer les frais, comme la caisse de médecins, ont accès dans le cadre de leur activité aux fiches de prestations, soit à des données médicales et à leur contexte. Un médecin ou un hôpital qui collabore avec une telle organisation doit donc préalablement informer ses patients de ce traitement, et requérir leur consentement. La déclaration du patient devrait figurer sur un formulaire séparé. Le refus d'octroyer le consentement ne doit pas entraîner de préjudices ou être sujet à des conditions.

Il est bien clair que la caisse-maladie a besoin d'un décompte des prestations pour pouvoir calculer le montant à indemniser. Ce décompte ne doit cependant pas forcément être fait par la caisse des médecins (organe de décompte); il peut aussi être effectué par l'hôpital même. Les patients peuvent consentir à la communication de leurs données de santé personnelles soit par écrit, soit oralement, selon la situation. Ils doivent cependant prendre leur décision de plein gré et sans qu'aucune pression n'ait été exercée.

De plus, ils doivent avoir la possibilité de biffer certains passages de la déclaration de consentement. Les critères suivants sont également applicables ici: le consentement n'est valable que si la patiente ou le patient a été clairement informé sur la portée du traitement de données, sur son but ainsi que sur les personnes à qui les données sont transmises. Cela signifie que les déclarations de consentement à caractère global telles qu'on les trouve souvent sur des formulaires de contrats d'assurance ou dans des conditions générales doivent être considérées comme nulles.

1.5.4 Externalisation de données médicales

Le feuillet thématique «Externalisation de la facturation par un médecin» est actuellement en cours de remaniement dans nos services. Cela demandera encore du temps, car quelques questions fondamentales en relation avec l'admissibilité d'un traitement de données par un tiers (externalisation) doivent encore être tirées au clair. La dernière révision de la LPD a introduit un nouvel article 10a. Celui-ci stipule que le traitement de données par un tiers est en principe admissible lorsqu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit. Les médecins sont cependant soumis à une obligation légale de garder le secret (secret médical selon l'art. 321 CP). Dans le cas présent, l'interdiction d'une externalisation du point de vue de la protection des données interdirait clairement l'externalisation de la facturation par un médecin sans le consentement explicite de la patiente ou du patient. L'ensemble des questions qui se posent, notamment en ce qui concerne la qualification du personnel auxiliaire, avec des réponses qui auront des conséquences importantes pour toutes les formes d'externalisation dans le domaine des obligations légales contractuelles de garder le secret, nous a incités à demander un avis écrit à l'Office fédéral de justice. Nous continuerons à traiter le sujet de l'externalisation en fonction de cette prise de position, en collaboration avec les autorités cantonales de protection des données.

1.5.5 Feuillet thématique «Lettres de sorties et rapports opératoires»

Nous avons dû adapter légèrement le feuillet thématique «Lettres de sorties et rapports opératoires», car le Tribunal fédéral a concrétisé par un arrêt les droits des assureurs concernant les lettres de sorties et les rapports opératoires. En principe, nous nous en tenons cependant à une communication progressive des informations à l'assureur. Le feuillet thématique est accessible sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des données – Feuillets thématiques.

1.5.6 Envoi d'échantillons de sang à l'étranger

Lorsqu'une société envoie des échantillons de sang pour analyse de Suisse en Afrique du Sud, elle doit assurer une protection adéquate des données par un contrat conclu avec le laboratoire sud-africain.

Une société sise en Suisse nous a contactés au sujet d'un projet de recherche prévoyant l'envoi d'échantillons de sang en Afrique du Sud pour analyse. Les échantillons de sang sont envoyés au laboratoire munis des initiales (prénom et nom) et d'un

numéro d'identification. La société voulait savoir s'il était impératif de conclure un contrat avec le laboratoire sud-africain. Dans ce contexte, il fallait d'abord examiner si un échantillon de sang avec les identificateurs mentionnés constitue encore une donnée personnelle. Le sang ou de manière générale des échantillons de cellules contiennent l'ADN du sujet à examiner. L'ADN comporte des informations sur une personne identifiable.

Nous sommes ainsi parvenus à la conclusion qu'en combinaison avec les identificateurs mentionnés, un échantillon de sang constitue bien une donnée personnelle. La société envoie régulièrement des données personnelles dans un pays qui n'assure pas une protection adéquate des données. Nous avons par conséquent transmis à la société suisse l'information qu'elle devait conclure avec le laboratoire en Afrique du Sud un contrat qui garantit aux personnes concernées une protection adéquate de leurs données personnelles.

1.5.7 Statistique sur les revenus des médecins indépendants

Un affinement subséquent d'une statistique peut mener à une situation où il serait à nouveau possible d'établir un lien entre les données et les personnes concernées. Cela reviendrait à modifier les exigences en matière de protection des données. En rapport avec une demande qui nous a été adressée concernant les statistiques régulières sur les revenus des médecins indépendants, il s'agissait de reconnaître et d'éviter le problème des petits nombres.

Depuis les années 70, la FMH élabore une statistique sur les revenus des médecins indépendants. Elle a récemment décidé d'affiner cette statistique. L'entreprise mandatée nous a contactés en nous priant d'examiner si ceci pouvait créer des problèmes du point de vue de la protection des données. L'affinement de l'analyse entraîne un effet problématique du point de vue de la protection des données, à savoir celui du petit nombre de cas.

Par des croisements de variables, on obtenait parfois des tableaux croisés qui contenaient moins de 20 observations ($N < 20$). Cela impliquait qu'il aurait été possible dans la statistique dont il est question d'attribuer certaines données à des personnes concernées. Cet état de fait aurait signifié que l'on n'avait plus affaire à des données statistiques non personnelles, ce qui aurait complètement changé les exigences en matière de protection des données. L'entreprise mandatée a proposé de fixer la valeur limite à $N > 20$ pour l'analyse statistique, ce qui est à notre avis suffisant.

1.5.8 Projet de recherche médicale dans un hôpital

Dans de nombreux projets de recherche médicaux, nous devons malheureusement constater que les charges ne sont pas entièrement appliquées. Dans la plupart des cas, les mesures de sécurité ne correspondent pas à l'état actuel de la technique. En outre, l'information aux patients sur le droit d'opposition et de veto, ainsi que l'obtention du consentement pourraient être améliorés.

Une partie de nos tâches consiste à contrôler l'application des charges que la Commission d'experts du secret professionnel en matière de recherche médicale impose pour l'attribution d'autorisations particulières ou générales. Nous avons choisi pour le contrôle un hôpital bénéficiant d'une autorisation générale. Celle-ci permet à l'hôpital d'effectuer des projets de recherche avec des données de patients internes, sans avoir à demander chaque fois une autorisation particulière auprès de la commission d'experts. Les charges suivantes sont applicables:

- Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées. Le processus de recherche entier y est pris en compte, de la collecte des données personnelles jusqu'à leur anonymisation ou leur effacement.

  Dans le cas examiné, les données des patients sont stockées dans deux archives sur papier. Les archives à court terme comportent les dossiers actifs des deux années précédentes, période au-delà de laquelle ils sont transférés aux archives à long terme, à la cave. Un photocopieur se trouve également dans les archives à court terme. La porte donnant sur les archives à court terme est en outre maintenue ouverte par une cale. La plupart des personnes travaillant à cet étage utilisent très probablement le photocopieur pour accomplir leurs tâches quotidiennes, et non pour accéder aux informations des archives. Nous avons émis des objections à cela et attiré l'attention sur le fait que le photocopieur devrait être placé en dehors du local des archives pour des raisons de confidentialité, de manière que seules les personnes autorisées puissent accéder aux dossiers de patients archivés. De plus, nous avons également signalé que le photocopieur pourrait prendre feu, ce qui entraînerait avec une grande probabilité la destruction des dossiers de patients archivés. Nous avons constaté en outre que les locaux d'archivage sont marqués en conséquence sur les portes d'entrée. Nous considérons cela comme dangereux, car une personne non autorisée sait ainsi immédiatement où se trouvent les dossiers de patients archivés dans un hôpital.

L'identification des dossiers de patients nécessaires pour un projet de recherche s'effectue par le code de diagnostic (CIM-10) ou par le code d'intervention chirurgicale (CHOP). Ceux-ci sont accessibles par voie informatique à l'aide d'un tiers et permettent d'identifier le dossier recherché. Le chercheur peut ainsi collecter les données requises dans les dossiers médicaux. Afin que l'identification des patients ne soit plus possible directement dans le projet de recherche au moyen du nom, du prénom et de l'adresse, les données nécessaires sont transférées dans un fichier Excel à l'aide d'un pseudonyme. Le pseudonyme se compose des initiales du nom et prénom, ainsi que de la date de naissance. Nous avons signalé que le choix d'un tel pseudonyme ne peut pas être considéré comme conforme à la protection des données. Des solutions complètes dans le domaine de la pseudonymisation se trouvent dans la publication «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin» des auteurs Reng, Debold, Specker et Pommerening (mars 2006).

La réalisation du travail de recherche s'effectue à l'aide de données pseudonymisées, stockées sur PC dans un fichier Excel. L'accès au PC est possible à l'aide d'une identification d'utilisateur et d'un mot de passe. Nous considérons cela comme suffisant si l'identification de la personne n'est possible que par un pseudonyme. Si le tableau liant les pseudonymes aux identifications se trouve également sur le PC, ce tableau doit être protégé conformément à l'état actuel de la technique. Cela signifie dans le cas présent que pour un PC non interconnecté (stand-alone), le tableau peut être protégé notamment par de bons procédés de chiffrement. Par contre, si le PC est connecté en réseau, l'identification d'utilisateur et le mot de passe ne sont plus suffisants. En plus du mot de passe, il faut alors recourir par exemple à une carte à puce, qui est protégée contre l'interception du mot de passe ou du NIP par un enregistreur de frappes.

- Selon une autre charge liée à l'autorisation générale, l'hôpital ne peut réaliser aucun projet de recherche sans approbation de la commission cantonale d'éthique et certaines informations sur les projets de recherche doivent être collectées et transmises une fois par année au secrétariat de la Commission d'experts du secret professionnel en matière de recherche médicale.

  Selon les indications de l'hôpital, aucun projet de recherche n'a été réalisé sans l'approbation de la commission cantonale d'éthique. Nous avons cependant observé que certaines données qui doivent être remises une fois par année au secrétariat de la commission d'experts n'ont pas été collectées.

- Une autre charge consiste en ceci que l'hôpital doit renseigner systématiquement ses patientes et patients sur le fait que les données personnelles peuvent être utilisées à des fins de recherche et que cette utilisation peut être refusée (droit de veto).

  Nous avons fait observer aux responsables que, dans la brochure d'information destinée aux patients, il manque encore l'indication qu'ils ont un droit d'opposition ou de veto s'ils ne veulent pas que leurs données soient utilisées à des fins de recherche.

1.5.9 Collecte de données de patients pour la recherche médicale

Nous avons constaté que les hôpitaux bénéficiant d'une autorisation générale de la commission d'experts dérogeant au secret professionnel dans la recherche médicale sont, dans de nombreux cas, faussement partis du principe qu'ils ne devaient pas obtenir de consentement auprès des patients concernés pour les travaux de recherche. Avec une autorisation générale, il n'est pas nécessaire d'obtenir le consentement uniquement lorsque cela serait disproportionnellement difficile, impossible ou inacceptable.

61 Plusieurs contrôles ont montré que les chercheurs dans les hôpitaux partent du principe qu'il n'est pas nécessaire d'obtenir une autorisation auprès des patientes et patients concernés lorsque la recherche porte sur des données qui sont enregistrées ou archivées au sein de l'hôpital, dans la mesure où l'hôpital est en possession d'une autorisation générale de la Commission d'experts en matière de recherche médicale.

Cette interprétation ne correspond cependant pas aux dispositions normatives. C'est uniquement lorsqu'il est disproportionnellement difficile, impossible ou inacceptable pour les chercheurs d'obtenir le consentement des personnes concernées (ou de leur représentant légal, de leurs proches), que l'on peut procéder à des recherches avec les données personnelles en question sur la base de l'autorisation générale.

Impossible ou disproportionnellement difficile signifie par exemple que la personne concernée, son représentant légal ou les proches ne peuvent pas être trouvés. Par ailleurs, il s'agit également de considérer que l'obtention d'une autorisation auprès des personnes concernées peut être inacceptable.

Cela peut être le cas lorsqu'une nouvelle confrontation des personnes concernées avec une situation difficile entraînerait une forte charge émotionnelle, comme le souvenir d'une lourde maladie passée ou d'un suicide dans la famille. C'est dans de tels

cas seulement qu'il est possible d'effectuer des recherches sans le consentement des personnes concernées sur la base d'une autorisation générale de la commission d'experts.

Il a été de plus en plus souvent affirmé ces derniers temps que les données pour la recherche ne devaient pas être effacées, car des conclusions importantes pour la descendance pourraient éventuellement en être tirées par la suite. Il est aussi souvent répété qu'en cas de données existantes, on ne peut ou ne doit plus obtenir des autorisations pour de nouveaux objets de recherche, notamment en raison des ressources beaucoup trop élevées. Une telle démarche n'est cependant pas conforme à la protection des données. Plus les données personnelles à traiter sont sensibles, plus les personnes concernées doivent être informées en détail sur le traitement de données, afin qu'elles puissent comprendre à quoi précisément elles donnent leur consentement (but, étendue du traitement de données, quand intervient l'effacement des données personnelles collectées, etc.). Si la personne concernée se fait une idée fausse du consentement, celui-ci n'est pas valable.

Une autre solution possible consiste à constituer des systèmes qui mettent des données anonymes à disposition des chercheurs. Cela s'effectue dans de nombreux cas par le recours à des pseudonymes. Si les pseudonymes et les informations identifiantes correspondantes sont gérés en sécurité par un tiers de confiance (Trusted Third Party, TTP), on peut admettre que le chercheur travaille avec des données anonymisées. Dans de tels cas, une autorisation ne serait pas nécessaire. Ce n'est que pour une éventuelle identification des personnes pour le projet de recherche qu'il faudrait une autorisation. Des approches possibles se trouvent dans la série de publications de la «Telematikplattform für Medizinische Forschungsnetze» sous la référence «Generische Lösungen zum Datenschutz für Forschungsnetze in der Medizin / Generische Datenschutzkonzepte» des auteurs Reng, Debold, Specker et Pommerening, de mars 2006 (voir p. ex. sur le site web www.tmf-net.de, sous «Produkte und Services»).

1.6 Assurances

1.6.1 Case management (Gestion des cas)

Des données personnelles sensibles sont traitées dans le cadre du case management (gestion des cas). Du fait que les gestionnaires de cas agissent tant dans l'intérêt du mandant que dans celui de la personne concernée et que des conflits d'intérêts peuvent en résulter, les principes de la finalité et de la transparence doivent être scrupuleusement respectés.

Le case management (gestion des cas) est appliquée par différents organismes. Ce contexte a ceci de particulier que les gestionnaires de cas d'une part interviennent pour le compte d'assurances ou d'employeurs afin de maintenir aussi bas que possible les coûts résultant d'un accident ou d'une maladie, d'autre part doivent autant que possible aider les personnes concernées à réintégrer le processus de travail. Il est évident qu'un conflit d'intérêts peut survenir entre les objectifs de l'assurance ou de l'employeur et ceux de la personne concernée. Pour que le gestionnaire de cas puisse procéder de manière légale au traitement des données, il est particulièrement important qu'il informe la personne concernée sur son rôle, ses objectifs, le but du traitement de données et son mandant. De plus, les données personnelles ne peuvent être utilisées que pour des finalités reconnaissables pour la personne concernée. Les gestionnaires de cas ne peuvent donc pas dans une situation difficile se présenter comme «bienfaiteur», mais doivent veiller à la transparence – aussi sur le fait que leur activité peut le cas échéant ne pas être à l'avantage de la ou des personnes concernées.

1.6.2 Enregistrement des fichiers des caisses-maladie

Les assurances-maladie obligatoires sont considérées comme des autorités fédérales et doivent nous déclarer leurs fichiers ou désigner un responsable de la protection des données. Manifestement, certaines incertitudes subsistent notamment auprès des petites caisses-maladie.

Les assureurs-maladie sociaux (selon la LAMal) reconnus sont considérés comme des autorités fédérales au sens de la LPD; en tant que tels il sont tenus de nous déclarer tous leurs fichiers. Ils peuvent se libérer de cette obligation en désignant un responsable de la protection des données, qui assure de manière indépendante l'application interne des dispositions relatives à la protection des données et tient un inventaire des fichiers. Une enquête menée en collaboration avec l'Office fédéral de la santé publique

(OFSP) a fait ressortir que quelques assureurs-maladie n'ont pas respecté leurs obligations légales. Nous avons pris contact avec les assureurs défaillants et les avons informés de leur obligation légale. Notre intervention a démontré que la désignation d'un responsable de la protection des données satisfaisant au critère de l'indépendance peut se révéler ardue pour les petites caisses-maladie. Malgré tout, une partie de ces assurances-maladie craignent en premier lieu l'enregistrement des fichiers. Manifestement, des craintes infondées subsistent sur la divulgation de données d'assurance. A la suite d'entretiens d'information personnels, quelques assurances ont encore opté pour la déclaration. Dans quelques rares cas, nous sommes encore en pourparlers, car leur situation ne se présente pas avec suffisamment de clarté en raison de reprises ou d'autres circonstances.

1.6.3 Étendue du droit d'accès aux dossiers dans la procédure LAA

Même en cas d'examen d'un droit à une rente, l'assureur peut exiger de consulter des pièces datant d'une période antérieure à l'octroi de la rente. Les conditions de la proportionnalité doivent être respectées à cet égard.

Suite à la demande d'un avocat, nous avons étudié la question de savoir s'il est admissible qu'un assureur accidents puisse, dans le cas d'une vérification de rente, consulter des dossiers médicaux provenant d'une période antérieure à l'octroi de la rente. L'avocat était d'avis qu'après l'octroi d'une rente, l'assureur-accidents n'était en droit de consulter que les dossiers constitués après la date d'octroi de la rente. Nous sommes arrivés à la conclusion que, même en cas d'examen d'un droit à une rente, la consultation de pièces provenant d'une période antérieure à l'octroi de la rente est proportionnée dans la mesure où les pièces sont significatives pour le cas concret. A cet égard, nous avons dû considérer que l'assureur-accidents trouve dans la LAA une base légale pour le traitement de données et que la personne qui fait valoir un droit à une rente aurait de toute manière été tenue de fournir toutes les informations requises pour l'évaluation du droit à la rente.

1.6.4 Feuillet thématique «Expertises demandées par les assureurs en responsabilité civile»

Nous avons adapté le feuillet thématique «Expertises demandées par les assureurs en responsabilité civile» à la législation actuelle. La demande d'une expertise par un assureur en responsabilité civile pour déterminer l'obligation de prise en charge est admissible même sans le consentement de la personne concernée. Les principes de

la finalité et de la transparence doivent cependant être respectés. L'assureur doit donc informer les personnes concernées de la demande d'expertise et du but du traitement de données que cela implique.

Le feuillet thématique est accessible sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des données – Feuillets thématiques.

1.6.5 Communication électronique de données en matière d'AVS/AI

L'Office fédéral des assurances sociales (OFAS) a l'intention de permettre aux caisses de compensation et aux offices AI des cantons d'accéder à la banque de données eRegress pour que ces services puissent traiter électroniquement les tâches qui leur sont déléguées dans le cadre des recours AVS/AI. Bien que nous comprenions le besoin de permettre d'accéder à ces données par le biais d'une procédure d'appel, nous n'avons pas pu donner notre feu vert car les organes fédéraux doivent respecter le principe de légalité. Le droit des assurances sociales en vigueur ne présente clairement pas les bases légales nécessaires. De même, les critères auxquels devrait satisfaire un projet-pilote ne sont pas remplis. Il faut donc créer la base légale formelle qui permettra la création de cette banque de données fédérale.

L'OFAS a délégué des tâches concernant les recours en matière d'AVS/AI aux caisses cantonales de compensation et aux offices AI des cantons. L'échange de données à cet effet se fait sur papier. Mais l'OFAS demande que désormais, les services cantonaux traitent électroniquement ces affaires de recours et dans ce contexte, entend leur permettre d'accéder à la banque de données eRegress, annoncée auprès du préposé fédéral. Cette banque de données a été mise au point par l'Office fédéral de l'informatique et de la télécommunication (OFIT), qui nous a soumis pour avis le résultat des investigations effectuées au niveau interne à l'OFAS.

Dans notre prise de position, nous avons certes confirmé l'existence d'une base légale concernant le traitement et la communication de données sous forme imprimée pour les recours AVS/AI. Par contre, nous avons constaté que l'accessibilité électronique, à savoir la communication de données par le biais d'une procédure d'appel, ne possédait aucune base légale. Le législateur impose aux organes fédéraux des exigences légales plus élevées pour l'accessibilité de données en ligne; en effet, le potentiel de risques pour les droits de la personnalité des personnes concernées y est plus élevé. Selon l'art. 19 al. 3 LPD, il faut une base légale prévoyant expressément la procédure d'appel; les données relatives à la santé requièrent même une loi au sens formel. Les

organes qui ont accès aux données doivent être expressément désignés, ainsi que les catégories des données consultables en ligne, les autorisations d'accès, les autorisations de traitement et le but de la consultation. Nous avons certes constaté à l'art. 14 de l'ordonnance sur la partie générale du droit des assurances sociales (OPGA) la présence d'une base légale pour l'externalisation de la tâche en question, mais pas pour la communication de données en ligne.

La gestion conjointe d'une banque de données conformément à l'art. 16 al. 2 LPD est à notre avis envisageable, mais nous avons toutefois souligné qu'une ordonnance du Conseil fédéral devait également s'appuyer sur la loi sur les assurances sociales; celle-ci aurait à réglementer la gestion commune de la banque de données automatisée dans les grandes lignes, alors que les détails pourraient être fixés dans l'ordonnance du Conseil fédéral. En outre, nous avons précisé que même pour une banque de données gérée conjointement, une base légale au sens formel était nécessaire et qu'une ordonnance ne suffisait pas. Pour conclure, nous avons estimé que les critères en vue de la réalisation d'un projet-pilote n'étaient pas remplis.

1.6.6 Permanence téléphonique dédiée aux abus de l'aide sociale

Un parti politique a publié un numéro de téléphone que les citoyens désirant dénoncer un abus de l'aide sociale pourront composer. Plusieurs questions d'ordre juridique se sont posées dans ce contexte. Nous estimons que la lutte contre l'abus en matière d'aide sociale répond certes à un intérêt public, mais le traitement de ces informations est la tâche exclusive des autorités compétentes.

Après avoir appris par la presse qu'un parti politique avait mis en service un nouveau numéro de téléphone par lequel les citoyens peuvent dénoncer d'éventuels abus en matière d'aide sociale, nous nous sommes prononcés sur cette question. Il s'agit plus précisément ici de savoir si des tâches de l'Etat peuvent être assumées par des particuliers sans mandat légal exprès. Il y a autorisation expresse pour les particuliers si conformément à l'intérêt public visant à lutter contre l'abus en matière d'aide sociale, ils informent directement les autorités compétentes. Il en va autrement lorsque la dénonciation est adressée à une institution privée. Nous avons constaté que la législation fédérale sur les assurances sociales ne contient aucune base légale permettant de déléguer ce genre de tâches de politique sociale à des particuliers. Indépendamment de la question de la base légale, une personne concernée par une dénonciation de ce type peut porter plainte contre l'institution privée pour atteinte illicite à la personnalité et demander en justice l'effacement des données enregistrées.

1.7 Secteur du travail

1.7.1 Protection des données dans le cadre de l'utilisation de l'infrastructure électronique de l'administration fédérale

L'administration fédérale ne dispose pas d'une base légale pour traiter les données liées à son infrastructure électronique. Un groupe de travail interdépartemental a élaboré un projet pour créer une telle base légale.

Pour accomplir ses tâches, l'administration fédérale a mis en place ces dernières années une infrastructure électronique (ordinateurs, réseaux, site en ligne, poste électronique, etc.). Les informations sont traitées sous forme électronique (par exemple les courriels) et l'utilisation de cette infrastructure génère toute une série de traces électroniques (par exemple les logfiles).

La quantité de données liées à l'utilisation de l'infrastructure électronique, y compris les copies de sauvegarde, est énorme et très souvent les données contenues sont liées à une personne identifiée ou identifiable (adresse personnelle de poste électronique, adresse IP, etc.). En outre, les données personnelles traitées peuvent être sensibles (par exemple le contenu des courriels privés, la liste des sites web visités, etc.).

Pour pouvoir traiter ce type de données, l'administration fédérale doit disposer d'une base légale formelle, qui n'existe pas encore. Du point de vue de la protection des données, cette situation n'est pas tolérable. Afin de remédier à cette lacune, un groupe de travail interdépartemental dirigé par l'Office fédéral de la justice (OFJ), impliquant l'Office fédéral de l'informatique et de la télécommunication (OFIT), le Département fédéral de justice et police (DFJP), l'Unité de stratégie informatique de la Confédération (USIC), la Chancellerie fédérale (ChF), l'Office fédéral du personnel (OFPER) et le PFPDT, a été créé.

Le premier projet de modification de la loi sur l'organisation du gouvernement et de l'administration (LOGA) prévoyait que l'administration fédérale pouvait, à certaines conditions, traiter toutes les données liées à l'infrastructure électronique qu'elle voulait. Le projet a été fortement critiqué lors de la consultation. Le groupe de travail a donc changé d'optique. Le second projet de modification de la LOGA prévoit une interdiction générale de traiter des données liées à l'infrastructure électronique, avec des exceptions. Du point de vue de la protection des données, cette seconde proposition est meilleure, car elle oblige les responsables de l'infrastructure électronique à déterminer quels traitements de données sont nécessaires.

1.7.2 Le contrôle de présence à l'aide des empreintes digitales

Une entreprise nous a demandé comment mettre en place un système de contrôle de la présence et de saisie du temps de travail des collaborateurs sur la base des empreintes digitales. Afin de limiter les risques de traitement de données biométriques, nous avons recommandé à l'entreprise de n'utiliser non pas les empreintes digitales elles-mêmes, mais seulement un extrait des images d'empreintes.

Les empreintes digitales, de même que les caractéristiques qui en sont extraites, sont des données biométriques. Elles constituent des particularités inhérentes d'une personne, en manifestent l'originalité et ne peuvent en principe pas être usurpées par des tiers. Les systèmes d'authentification biométriques limitent ainsi fortement les risques que comportent les cartes classiques de pointage tels que la perte, la copie ou le vol. Néanmoins, au lieu de l'empreinte digitale, il ne faudrait utiliser qu'un extrait de l'image d'empreinte afin de réduire les risques que le traitement de données biométriques implique au niveau de la sécurité. On sélectionne alors des caractéristiques précises de l'empreinte digitale clairement attribuables à une personne en particulier. Cette méthode permet de réduire le risque d'utilisation abusive des données et de garantir un contrôle sûr de la présence et de la saisie des temps des collaborateurs. Les extraits de l'image d'empreinte doivent en outre être enregistrés localement sur une carte à puce. Il n'est pas nécessaire de créer une base de données centrale rassemblant des données biométriques, qui serait exposée à divers risques au niveau de la sécurité.

Plusieurs entreprises ont posé des questions similaires au sujet de l'utilisation de données biométriques. Nous avons donc rédigé un «Guide relatif aux systèmes de reconnaissance biométrique», qui a été publié sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des Données – Brochures.

1.7.3 Logiciels espions au poste de travail

Au cours de l'année écoulée, nous avons à plusieurs reprises reçu des plaintes concernant l'utilisation de divers programmes informatiques permettant une surveillance absolument continue des collaborateurs sur leur lieu de travail. Dans tous les cas, nous avons réussi à convaincre les entreprises concernées de modifier cette pratique, conformément aux principes de la protection des données.

Une grande partie des plaintes concernait l'installation secrète d'un logiciel permettant une surveillance permanente de l'employé à son poste de travail. Ces programmes portent atteinte à la sphère privée de l'employé. L'employeur est certes tout à

fait autorisé à contrôler le travail fourni par son employé ainsi que les moyens informatiques mis pour cela à sa disposition (ordinateur, messagerie électronique, Internet, etc.). Il n'a toutefois pas le droit de surveiller les moindres faits et gestes de ses collaborateurs et doit respecter certaines règles. Ainsi, il doit d'une part énoncer clairement comment les moyens informatiques doivent être utilisés sur le lieu de travail (règlement d'utilisation). Il doit annoncer de manière claire que le respect du règlement peut être contrôlé et qu'une infraction à ce règlement peut être sanctionnée; il doit indiquer avec précision ce qui est contrôlé et par quels moyens.

Mis à part les prescriptions de la loi sur la protection des données, il faut aussi respecter les dispositions du droit du travail, qui n'autorisent pas la surveillance permanente et secrète sur le lieu de travail et la rendent même passible de sanctions.

Nous avons prié les entreprises concernées de modifier leurs pratiques conformément au droit de la protection des données et au droit du travail.

1.7.4 Allocations familiales et formulaire de demande

Au cours de l'année écoulée, nous avons approuvé l'introduction légale du registre des familles et n'avons formulé aucune objection à la base légale correspondante. Par la suite, nous avons reçu plusieurs demandes en relation avec les différents formulaires de demande et les données personnelles ainsi relevées. C'est pourquoi nous avons proposé d'uniformiser les formulaires de demande.

Après notre approbation de la base légale relative aux allocations familiales (voir notre 16e rapport d'activités 2008/2009, ch. 1.7.1) et l'entrée en vigueur de la loi le 1er janvier 2009, nous avons reçu de la part de la population diverses demandes concernant la sensibilité des données personnelles qui sont relevées dans les formulaires de demandes d'allocations familiales. Nous avons par la suite constaté de grandes disparités, quant au contenu, entre les différents formulaires servant à relever les données nécessaires à la demande d'allocations familiales. Vu que ces formulaires permettent de relever des données personnelles sensibles et que les pratiques des caisses d'allocations familiales varient selon les cantons, nous avons suggéré d'uniformiser les formulaires dans toute la Suisse. Nous avons proposé de réglementer le contenu matériel des formulaires de demande au niveau légal, à savoir dans la loi sur les allocations familiales. La mise en œuvre et l'application de cette loi relève certes de la responsabilité des organes cantonaux d'exécution. Mais à notre avis, l'uniformisation du contenu de ces formulaires ne touche pas cette compétence de surveillance cantonale.

1.7.5 Contrôle de santé pour les collaborateurs de la Poste

La Poste nous a présenté un projet de gestion de la santé visant pour l'essentiel la promotion de la santé, la gestion des absences ainsi que la gestion des cas d'accident ou de maladie. Certaines données médicales des collaborateurs seront traitées par l'employeur. Nous avons analysé ce projet et n'avons rien à lui objecter dans la mesure où, du point de vue de la protection des données, certaines conditions sont respectées.

Le projet de gestion de la santé de la Poste a pour objectif la promotion de la santé des collaborateurs, le traitement des cas d'accident et de maladie et la gestion des absences. En sa qualité d'employeur, la Poste traitera dans ce contexte les données médicales des collaborateurs, donc de données personnelles sensibles. Nous avons expliqué aux responsables qu'un projet de ce type, qui implique des mesures de prévention dans le domaine de la santé ne peut être mis en place, à l'exception du dépistage précoce prévu dans l'assurance invalidité, que dans le cadre des dispositions usuelles du droit du travail,. En effet, la loi ne prévoit pas une délégation à l'employeur des mesures prévues dans l'AI. Pour un tel projet de gestion de la santé, l'employeur a donc besoin du consentement des employés; et étant donné qu'il ne s'agit pas là à proprement parler de l'exécution d'un contrat de travail, il faut que les deux parties soient d'accord. Certes il incombe à l'employeur de remplir son devoir d'aide et d'assistance, qui englobe aussi la protection et la promotion de la santé, mais ce devoir se limite aux conditions et problèmes touchant à la technique de travail. Des dérogations sont envisageables, mais doivent rester des exceptions (p. ex. absences répétées et manifestes pour raisons de santé). Les autres mesures de soutien de l'employeur nécessitent en principe toujours le consentement des personnes concernées.

Le système de gestion de la santé dans une entreprise doit donc toujours reposer sur les consentements de l'employeur et de l'employé. Il convient à ce propos d'attirer explicitement l'attention de l'employé sur le caractère volontaire de sa participation au projet. La Poste a adapté son projet en fonction de nos remarques.

1.7.6 Règlement du personnel et règlement-vidéo de Lidl

Avertis par divers articles de presse, nous avons examiné au cours de l'année écoulée sur la pratique de l'entreprise Lidl en matière de vidéosurveillance et de fouille des collaborateurs sur leur lieu de travail. Nous avons constaté que l'information transmise aux collaborateurs était insuffisante. Par contre, les données des collaborateurs étaient traitées conformément à la protection des données.

Selon divers articles de presse, Lidl ne se conformerait pas aux prescriptions de la protection des données en matière de vidéosurveillance et de fouille des collaborateurs sur leur lieu de travail. Nous avons donc demandé à l'entreprise un supplément d'informations sur le traitement des données des collaborateurs. Nous avons ensuite analysé le projet de protection des données, le règlement du personnel et la déclaration de vidéosurveillance de l'entreprise. Il est ressorti de notre examen que les informations à transmettre aux collaborateurs au sujet de la vidéosurveillance et de la fouille devaient être précisées. L'entreprise Lidl a procédé aux modifications nécessaires que nous avons proposées.

1.7.7 Contrôle des collaborateurs sur Internet

Une forte concurrence règne sur le marché des renseignements économiques et des informations sur la solvabilité. Elle force les entreprises à innover constamment. Une agence de renseignements en matière de solvabilité proposait à des responsables du personnel, moyennant rémunération, des données concernant la solvabilité de futurs collaborateurs ou de collaborateurs déjà employés. Le Tribunal administratif fédéral a admis notre requête de mesures provisionnelles concernant ce service.

Par le biais de son service «Mitarbeiter Check» (Contrôle des collaborateurs), une agence de renseignements en matière de solvabilité sise en Suisse projetait, dans le but d'élargir son carnet de clients, de vendre des informations concernant la solvabilité de collaborateurs à des responsables de services du personnel. Nous avons eu connaissance du projet encore avant la mise en fonctionnement de ce service, sur la base des nombreux courriels de publicité diffusés par l'agence. Les données des collaborateurs jouissant d'une protection particulière en vertu de l'art. 328b CO, nous sommes intervenus immédiatement auprès du Tribunal administratif fédéral et avons demandé d'ordonner une mesure provisionnelle afin de faire cesser immédiatement cette offre de prestation. Le Tribunal administratif fédéral a admis notre requête, interdit ce service sur la base d'une décision provisoire et nous a priés d'émettre une recommandation dans un délai de trois mois. L'agence de renseignements a par la suite annoncé qu'elle abandonnait définitivement son projet.

1.7.8 La remise de certificats de caisses de pension

La pratique des institutions de prévoyance qui remettent les certificats personnels de caisse de pension de leurs assurés aux employeurs ne respecte ni le principe de légalité, ni le devoir de discrétion attaché au droit des assurances sociales. Une institution de prévoyance ayant rejeté notre recommandation, nous avons déposé une demande de décision sur laquelle le Département fédéral de l'intérieur aura à se prononcer.

Nous avons appris qu'une caisse de pension envoie les certificats personnels de ses assurés à une adresse indiquée par l'employeur. Celui-ci distribue ensuite les certificats non adressés personnellement à ses employés et a ainsi la possibilité de prendre connaissance de leur contenu.

Nous sommes d'avis que cette pratique de remise indirecte est illicite. Cette institution de prévoyance privée, agissant en qualité d'organe fédéral, est liée par le principe de légalité lorsqu'elle traite des données. Elle ne doit donc communiquer des données que si cette communication repose sur une base légale. Aucune base légale ne justifie une communication de données des employés assurés chez elle à leurs employeurs. En outre, la loi fédérale sur la prévoyance vieillesse, survivants et invalidité (LAVS) prévoit clairement la manière dont la communication de données doit avoir lieu pour respecter le devoir de discrétion.

Comme aucun accord n'a pu être trouvé avec l'institution de prévoyance malgré une correspondance abondante, nous avons émis une recommandation. Conformément à celle-ci, l'institution de prévoyance doit tout d'abord mettre fin immédiatement à l'envoi des certificats de caisse de pension des employés à leur employeur. Ensuite elle doit, lors de l'envoi des certificats, veiller à ce que les documents parviennent directement et exclusivement à la personne assurée. L'institution de prévoyance a rejeté notre recommandation. Du fait que celle-ci agit en qualité d'organe fédéral, nous avons, conformément à la procédure de surveillance des organes fédéraux, déposé une demande de décision auprès du Département fédéral de l'Intérieur (DFI) le 27 août 2009.

Nous estimons que l'institution de prévoyance ne peut invoquer ni l'art. 86b LPP, ni l'art. 331 al. 4 CO, pas plus que l'art. 89bis al. 2 CC à titre de base légale. En outre, nous ne voyons pas dans quel but de prévoyance professionnelle l'employeur aurait besoin des données personnelles de prévoyance et éventuellement des données concernant la santé de ses employés; la communication de données est ainsi aussi contraire au

but poursuivi en vertu de l'art. 86a al. 5 LPP. Enfin, également sous l'angle de l'art. 328b CO, l'employeur ne doit pas avoir connaissance de la situation patrimoniale personnelle et des données concernant la santé de son employé.

Par conséquent, on suppose que la caisse de pension ne respecte pas le principe de légalité puisqu'elle communique des données à un tiers sans base légale. Du fait que l'institution de prévoyance ne peut se fonder sur aucune exception légale pour la communication de données, on suppose qu'il y a en outre violation du devoir de discrétion.

La décision du DFI est attendue. Elle pourra faire l'objet d'un recours devant le Tribunal fédéral administratif autant de notre part que de celle de l'institution de prévoyance en question.

La demande de décision au DFI (en version allemande) figure en annexe (ch. 4.1.5).

1.7.9 Le règlement du personnel de Publica

La caisse de pension de la Confédération a intégré ses propres dispositions en matière de protection des données pour son personnel dans son règlement du personnel. Nous avons émis quelques objections dans le cadre de la consultation des offices. Publica a accepté l'ensemble de nos remarques.

La caisse de pension de la Confédération, Publica, a décidé d'intégrer, pour son personnel, ses propres dispositions en matière de protection des données dans son règlement du personnel. Dans le cadre de la consultation des offices, nous avons constaté que le règlement reposait sur une base légale insuffisante. En outre, nous avons fait remarquer que le projet de test de personnalité et de test d'évaluation ne contenait pas d'obligation d'information et qu'il y manquait une disposition sur le délai de conservation de ces tests. Le règlement prévoyait en revanche une prolongation de délai illimitée pour la conservation des données. Par ailleurs, il ne fixait pas de délai pour le renvoi des documents de candidature. Les dispositions régissant l'accès aux données en procédure d'appel ne réglaient pas non plus clairement quels fichiers sont concernés, quelles sont les données disponibles, dans quel fichier et sous quelle forme, quel est leur but, qui a accès à ces données et qui est responsable. Enfin, nous avons constaté des imprécisions quant au traitement des données relatives à la santé.

Publica a accepté nos remarques et adapté le règlement en conséquence.

1.8 Economie et commerce

1.8.1 Obligation de déclarer pour les maîtres de fichiers étrangers

L'obligation de déclarer un fichier est une disposition de droit public s'appliquant selon le principe de la territorialité. Cette obligation existe pour des personnes privées lorsqu'elles traitent régulièrement des données personnelles sensibles ou des profils de la personnalité, ou lorsqu'elles communiquent régulièrement des données personnelles à des tiers.

Sur mandat d'une étude d'avocats sise à Zurich, nous avons établi une expertise sur l'obligation de déclarer des fichiers qui se trouvent à l'étranger. La demande de l'étude d'avocats s'explique par le fait qu'une partie du traitement des données s'effectue dans des hôpitaux en Suisse et que les données sont transmises à un serveur qui se trouve aux Pays-Bas, aux mains d'une société belge. L'obligation de déclarer un fichier selon l'art. 11a LPD est une disposition de droit public s'appliquant selon le principe de la territorialité. L'obligation de déclarer se limite donc à des faits établis en Suisse. Comme il n'y avait, dans le cas présent, ni de traitement régulier de données personnelles sensibles ou de profils de la personnalité effectué en Suisse, ni de communication régulière de données à un tiers, nous sommes parvenus à la conclusion qu'il n'y avait pas d'obligation de déclarer le fichier se trouvant aux Pays-Bas, même si une partie du traitement des données intervient en Suisse.

1.8.2 Commentaires relatifs à la transmission de données en cas de fusion d'entreprises

Les fusions d'entreprises sont régulièrement à l'ordre du jour dans la vie économique. Il va de soi qu'elles s'accompagnent toujours de traitements de données à caractère personnel. Au cours des divers processus de réorganisation et de fusion, des données personnelles sont transmises et traitées de diverses manières; le risque existe que des personnes non autorisées aient accès à des informations à caractère personnel, que trop de données soient communiquées (qu'elles soient communiquées trop tôt ou aux mauvaises personnes) ou que des données personnelles soient soudain utilisées dans un but autre que celui prévu à l'origine. Or la loi sur la protection des données est applicable à tous les cas de fusion d'entreprises et à toutes les étapes de la fusion. Nous avons circonscrit ces risques et nous recommandons des mesures permettant d'éviter les atteintes à la personnalité. Ces commentaires se trouvent à l'annexe 4.1.4. Ils peuvent également être consultés sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Entreprises.

1.8.3 Explications concernant le conseiller à la protection des données en entreprise

La révision de la loi sur la protection des données, en vigueur depuis 2008, permet aux entreprises de pratiquer l'autorégulation. Ainsi, l'entreprise qui nomme un responsable de la protection des données et qui en informe le préposé fédéral est dispensée de l'obligation de nous déclarer ses fichiers. La position et le choix de la personne responsable de la protection des données doivent toutefois répondre à des critères déterminés. Elle doit avoir pour tâche principale de contrôler le traitement de données personnelles dans l'entreprise, si nécessaire de le corriger, et de tenir une liste de tous les fichiers disponibles. Pour mener à bien cette tâche de surveillance, le conseiller (ou la conseillère) à la protection des données doit être indépendant: il ne doit exercer aucune autre activité, doit présenter l'aptitude professionnelle nécessaire (dans le domaine de la protection des données comme dans le domaine technique spécifique à l'entreprise), doit pouvoir travailler sans être lié par des instructions et on ne peut le sanctionner à cause de ses activités. En outre, il doit avoir bien entendu accès à tous les fichiers, tous les traitements de données et toutes les informations nécessaires. Ces commentaires se trouvent à l'annexe 4.1.3. Ils peuvent également être consultés sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Entreprises.

1.8.4 Communication de données des membres d'une association sportive à des fins de marketing

Une fédération sportive suisse a demandé à ses clubs une liste de tous leurs membres. Ces données devaient être vendues à des fins de marketing. Plusieurs clubs nous ont demandé si cette manière de faire était correcte et s'ils avaient le droit de transmettre ces données personnelles. Nous leur avons expliqué qu'ils avaient besoin, pour transmettre ces adresses, du consentement des personnes concernées et nous avons enjoint la fédération d'attirer l'attention des clubs sur la situation juridique et de n'utiliser en aucun cas les données déjà livrées. Le recueil du consentement de chaque membre pourrait cependant être externalisé par les clubs et être confié à la fédération.

Une fois de plus, nous avons dû nous pencher sur le problème de la transmission d'adresses et autres données personnelles de membres d'un club à des tiers (p. ex. à des sponsors) à des fins de marketing (voir notre 16e Rapport d'activités 2008/2009, ch. 1.8.5). Les clubs ne doivent transmettre des données personnelles à des tiers que

si cette communication est reconnaissable pour la personne concernée et si celle-ci donne son consentement ou n'a pas manifesté son désaccord. Les clubs peuvent prévoir cette communication dans leurs statuts ou recueillir le consentement dans le cas d'espèce. En outre, les personnes concernées doivent être informées du fait qu'elles peuvent en tout temps s'opposer à ce genre d'utilisation de leurs données personnelles à des fins de marketing. Au printemps 2009, une fédération sportive suisse a écrit à ses clubs et, se fondant sur ses statuts, leur a demandé une liste de tous leurs membres (y compris les adresses postales et électroniques). Ces données devaient être utilisées à des fins de marketing. En outre, la fédération a mentionné que la transmission des données à des tiers (par la fédération) répondait absolument aux prescriptions de la LPD.

Par la suite, plusieurs clubs régionaux nous ont demandé si cette manière de faire était correcte. Ils voulaient savoir en particulier s'ils pouvaient ou même devaient transmettre les données personnelles souhaitées par la fédération. Nous avons attiré l'attention des clubs sur le fait qu'ils ne devaient transmettre les données de leurs membres que s'ils avaient pour cela le consentement de chaque membre. En cas de données non spécialement sensibles, un consentement implicite suffit avec une possibilité de opt-out. Dans tous les cas, il faut communiquer à la personne concernée le destinataire et le but de la communication des données et lui octroyer un droit d'opposition. Nous avons souligné en outre que l'utilisation des adresses électroniques pour l'envoi de publicité de masse est soumise à la loi fédérale contre la concurrence déloyale (LCD) et présuppose entre autres un consentement *explicite* (option opt-in). Nous sommes par ailleurs intervenus auprès de la fédération: nous l'avons priée d'attirer l'attention de ses clubs sur la situation juridique réelle et de n'utiliser en aucun cas les données livrées par les clubs régionaux. En particulier, la fédération ne doit pas communiquer ces données à d'autres tiers tant qu'elle n'est pas sûre que la transmission par les clubs à la fédération a lieu conformément au droit (donc en particulier avec le consentement de chaque membre). Alors seulement la fédération est en effet autorisée à traiter et à transmettre ces données à des tiers.

A l'occasion d'une entrevue avec la fédération, celle-ci nous a informé que la mise en pratique de ces mesures posait souvent des problèmes car les clubs, pour la plupart, n'avaient ni les ressources, ni la volonté de demander un consentement à leurs membres. Nous avons alors proposé un procédé conforme à la LPD: les clubs pourraient demander à la fédération de recueillir le consentement des membres, dans le cadre d'une mesure d'externalisation. Néanmoins, la fédération ne peut dans ce cas utiliser les données d'adresses qu'une seule fois pour demander, au nom du club, le consentement en vue de l'utilisation des données en question par elle-même. Ensuite, la fédération ne doit traiter que les données personnelles pour lesquelles elle a obtenu le consentement des personnes concernées.

1.8.5 Service d'information sur la solvabilité des locataires

Suite à notre recommandation de décembre 2008 concernant le cas «Mieter Check», nous avons mené d'intenses discussions avec l'entreprise Deltavista SA concernant la mise en œuvre de cette recommandation. À l'occasion d'un contrôle ultérieur effectué à l'automne 2009, l'entreprise nous a présenté un système et remis des documents que nous avons jugés, dans la forme qui nous a été présentée, comme étant conformes aux règles de protection des données et à nos recommandations. Nous avons donc mis fin à la procédure de surveillance.

L'entreprise Deltavista SA propose une plateforme Internet du nom de «Mieter Check» (service d'évaluation des locataires), par le biais de laquelle des personnes autorisées peuvent consulter des informations sur la solvabilité et la situation économique de locataires potentiels. Les propriétaires peuvent ainsi contrôler les indications fournies par les intéressés et réduire le risque de non-paiement de leur loyer.

Dans sa version initiale, «Mieter Check» utilisait un score pour calculer la solvabilité d'un locataire potentiel; cette notation – entre 250 et 700 points et représentée graphiquement sur un axe horizontal en trois couleurs (rouge, jaune, vert) – évaluait non seulement les antécédents de paiement et la mobilité du locataire, mais aussi les antécédents de paiement de son entourage ainsi que des données sociodémographiques. En plus de ce score, divers autres éléments, tels que la solvabilité des membres de la famille, les relations d'entreprises négatives ou la durée moyenne de résidence à une adresse, étaient munis d'un feu de signalisation (rouge, jaune, vert). Tous ces feux étaient rassemblés en un feu de signalisation général déterminant le taux de solvabilité du locataire potentiel. Selon la couleur de ce feu, «Mieter Check» recommandait la conclusion d'un contrat de bail (vert), la recherche d'informations supplémentaires (jaune) et la non-conclusion du contrat (rouge).

Après avoir établi les faits en juin 2008, nous avons constaté que Deltavista SA avait procédé à des adaptations par rapport à la version initiale du «Mieter Check» et avait en particulier éliminé les connexions problématiques de données. Ainsi, le score et les données sociodémographiques ainsi que l'examen des listes noires ne faisaient plus partie de l'évaluation de la solvabilité de la personne concernée. A côté du feu de signalisation général, on pouvait voir un texte d'explication en surlignage et un commentaire des antécédents de paiement munis des lettres A, B, C et D. Le feu de signalisation général n'était rouge que si la personne en question présentait des antécédents de paiement négatifs ou si son statut (mineur, sous tutelle, décédé) s'opposait à la conclusion valable d'un contrat.

Toutefois, nous avons constaté encore des lacunes dans la version remaniée concernant la pertinence, en matière de solvabilité, des données offertes à la consultation (notamment l'évaluation des autres personnes habitant dans le même ménage et leur lien avec la solvabilité de la personne concernée), ainsi que concernant la garantie du droit à l'information et du droit à l'effacement des données. Pour cette raison, le 16 décembre 2008, nous avons émis une recommandation (voir notre 16e Rapport d'activités 2008/2009, ch. 1.8.4).

Au terme d'intenses discussions avec l'entreprise Deltavista SA concernant la mise en œuvre de cette recommandation, nous avons procédé à une vérification à l'automne 2009. Dans le système qui nous a été montré, seules les données de la personne concernée sont intégrées dans l'évaluation de la solvabilité. Tant les clients que les personnes concernées sont désormais informés de la même manière sur les éléments pris en compte dans l'évaluation. En outre, l'entreprise donne des explications sur la manière dont les antécédents de paiement sont pris en compte et précise que le rapport de solvabilité est actualisé tous les jours car il est sujet à des modifications constantes; ainsi une décision ne devrait en général pas se baser seulement sur l'évaluation des feux de signalisation.

La personne faisant valoir son droit d'accès dispose des mêmes informations que le client consultant les données de solvabilité d'un locataire potentiel. Les feux de signalisation individuels et le feu de signalisation général ainsi que les autres informations sont transparentes pour la personne concernée et celle-ci peut voir quelles données sont traitées par l'entreprise dans le système «Mieter Check»; elle peut ainsi faire usage de son droit à la rectification et de son droit à l'effacement des données. Sur la base de la version qui nous a été montrée et des documents qui nous ont été remis, nous avons clos la procédure.

1.8.6 Examens auprès d'un fournisseur de tests génétiques

Dans le cadre d'un contrôle sur place, nous avons pu constater quelques défauts mineurs en matière de transparence chez un fournisseur de tests généalogiques et de paternité. Du fait que la société de Zurich a remédié sans délai aux défauts, nous avons renoncé à émettre une recommandation.

Sur la base de deux indications, nous avons procédé à un examen des faits dans une société à Zurich qui propose des tests de paternité et des analyses d'origine (tests généalogiques). Il était reproché à la société d'une part de ne pas effacer les résultats

de ces tests généalogiques malgré une demande de radiation des personnes concernées et d'autre part d'envoyer les échantillons ADN à une société aux États-Unis pour effectuer des tests. L'examen des faits s'est donc concentré sur l'enregistrement des données par la société zurichoise et la transmission d'échantillons de salive à une société américaine pour les analyses ADN dans le cadre des tests généalogiques. Nous avons également examiné le procédé relatif aux tests de paternité et n'avons pas pu constater d'infraction à la LPD.

L'examen des faits dans les bureaux de Zurich a démontré que la société satisfait autant que possible aux demandes de radiation des personnes concernées. Seules les données administratives des clients sont conservées, dans la mesure où cela est nécessaire pour la comptabilité.

En ce qui concerne la transmission à la société aux États-Unis d'échantillons ADN, nous avons constaté que l'information aux clients était lacunaire. Pour ces derniers, il était bien décelable sur le site web de la société qu'un tel échange de données aurait lieu; les clients n'en étaient cependant pas explicitement informés dans la convention. En conséquence de notre intervention, la société a corrigé ce défaut et a adapté aussi bien le site web que la convention d'analyse.

L'examen des faits a en outre démontré que la société zurichoise n'avait pas conclu de contrat écrit avec la société aux États-Unis pour l'analyse des échantillons ADN. La sécurité des données n'était donc pas suffisamment assurée. La société a immédiatement corrigé cette lacune suite à notre intervention. Nos recherches ont cependant montré que la société partenaire était certifiée «Safe harbor» aux États-Unis. La société zurichoise n'avait cependant pas connaissance de ce fait.

En résumé, le reproche qu'un traitement de données aurait été effectué malgré une demande de radiation n'a pas pu être confirmé. En ce qui concerne l'échange de données avec la société aux États-Unis, nous avons constaté des défauts mineurs, qui ont cependant été corrigés sans délai par la société zurichoise. Toute autre démarche était donc superflue de notre part.

1.9 Finances

1.9.1 Protection des données dans le trafic international des paiements (SWIFT)

Suite au conflit concernant l'accès des Etats-Unis à des données de transactions financières qui étaient enregistrées sur les serveurs du prestataire de services financiers SWIFT, ce dernier a ouvert en Suisse deux nouveaux centres opérationnels. Cette mesure devrait permettre de répondre à nos préoccupations et à celles des autorités européennes en matière de protection des données. En outre, les Etats-Unis ont passé avec l'Union européenne (UE) une convention devant permettre, dans le cadre de la lutte contre le terrorisme international, l'accès aux données SWIFT enregistrées dans l'UE.

La majeure partie des transactions financières et des transactions sur titres opérées au niveau international se déroulent par l'intermédiaire de SWIFT. A cet effet, ladite société exploitait jusqu'ici deux centres opérationnels qui enregistraient et traitaient des données identiques, l'un en Belgique, l'autre aux Etats-Unis. Les autorités américaines ont accès au centre situé aux Etats-Unis, dans le cadre des procédures en cours touchant à la lutte contre le terrorisme.

Etant donné que toutes les données de SWIFT étaient enregistrées dans ce centre, les autorités américaines avaient donc accès à des données n'ayant aucun rapport direct avec les USA (p. ex. des données concernant des virements intra-européens ou même, plus rarement, des virements effectués par l'intermédiaire de SWIFT à l'intérieur des frontières suisses).

Dans ce contexte, la société SWIFT a décidé que désormais, elle n'enregistrerait les données de transactions purement européennes qu'en Europe, à savoir en Belgique et en Suisse. A cet effet, elle a ouvert deux nouveaux centres de calcul en Suisse. Elle entend ainsi retirer aux Etats-Unis l'accès aux transactions financières qui se déroulent soit à l'intérieur des frontières européennes, soit à l'intérieur des frontières suisses. Nous approuvons la création de ces centres en Suisse.

En réaction à ces développements, les Etats-Unis ont négocié un accord avec l'UE dont le but serait de permettre aux autorités américaines de lutte anti-terrorisme d'accéder à des données concernant la zone européenne. Cette convention a été toutefois rejetée par le Parlement européen en février 2010. Reste encore à savoir si l'UE et les Etats-Unis négocieront un nouvel accord à une date ultérieure.

1.9.2 Conventions de double imposition

Les banques suisses ont été sous le feu des critiques internationales au sujet du secret bancaire et d'une prétendue aide à l'évasion fiscale. La Suisse pour sa part a été placée par l'OCDE sur une «liste grise» dans le cadre de la lutte contre les paradis fiscaux. Dans ce contexte, le Conseil fédéral a décidé de s'écarter de sa position actuelle dans les cas d'évasion fiscale et de passer avec certains Etats des contrats bilatéraux garantissant une coopération renforcée en matière de fraude fiscale.

La législation suisse fait une distinction entre évasion fiscale et fraude fiscale. L'entraide judiciaire internationale n'étant généralement pas accordée dans les affaires d'évasion fiscale, la Suisse a été qualifiée de «paradis fiscal» et placée par l'OCDE sur une «liste grise». A la suite de cela, le Conseil fédéral a décidé de négocier une série d'accords bilatéraux avec un certain nombre d'Etats.

En substance, ces accords permettent aussi de faire appel à l'entraide judiciaire internationale dans les cas d'évasion fiscale. Les conditions requises sont que l'Etat requérant ait épuisé les voies de droit à l'intérieur de ses frontières et qu'il puisse présenter des indices concrets d'évasion fiscale. La recherche de preuves tous azimut ou par «fishing expeditions» – telle que la recherche par quadrillage – est toutefois explicitement exclue.

Nous avons examiné les accords négociés et conclu qu'ils constituent une base légale suffisante pour permettre une collaboration avec les autorités fiscales étrangères. Néanmoins, nous nous permettons de souligner que les demandes d'Etats étrangers augmenteront et que de ce fait, les échanges de données personnelles entre autorités augmenteront aussi.

1.9.3 Protection des données dans la cession transfrontière de créances

Une start-up nous a contactés à propos des diverses questions de protection des données qui se posent en cas de cession de créances hors frontières. Du point de vue de la protection des données, il convient de faire la différence entre la cession de créances et le recouvrement car ces deux domaines sont soumis à des exigences différentes de la LPD.

La loi fédérale sur la protection des données (LPD) distingue nettement la communication de données à des tiers (art. 3 let. f LPD) et le traitement de données par un tiers (art. 10a LPD, externalisation). Dans le cas du recouvrement de créances, le créancier

mandate un tiers pour le recouvrement de sa créance. L'entreprise de recouvrement est en général liée par les directives du mandant (créancier), qui conserve le pouvoir de décision sur la créance. Il s'agit dans ce cas d'un «traitement de données par un tiers» conformément à l'art. 10a LPD et le créancier doit assumer la responsabilité des activités de l'entreprise de recouvrement et peut être tenu pour responsable de ses éventuelles violations des règles de protection des données.

Lors de la cession de la créance, la créance passe des biens du créancier initial (le cédant) à ceux du nouveau créancier (le cessionnaire). Le cédant perd de ce fait le pouvoir de disposition sur la créance, il ne peut donc ni faire valoir la créance cédée, ni la céder encore une fois. Le cessionnaire ne se trouve cependant pas dans une relation de mandat avec le cédant, mais a acquis la créance et peut donc décider lui-même de ce qu'il en advient ultérieurement. Du fait qu'il peut faire valoir la créance dans son propre intérêt, la différer ou la remettre, le traitement de données que ces démarches impliquent n'est plus un traitement de données par un tiers (externalisation), mais une communication de données à des tiers (conformément à l'art. 3 let. f LPD) opérée par le cédant. Dans ce contexte, après la cession de créance, le cédant ne peut plus être tenu responsable des violations des règles de protection des données du cessionnaire.

Dans la perspective d'un transfert de données vers un pays qui ne dispose pas d'un niveau de protection des données adéquat conformément à l'art. 6 al. 1 LPD, le cédant peut invoquer l'art. 6 al. 2 let. c LPD. Une relation de contrat lie le cédant et le débiteur, selon laquelle le débiteur doit fournir au créancier le montant dû. Au cas où rien d'autre n'est convenu dans le contrat, le cédant est libre de vendre cette créance à un tiers (le cessionnaire); mais il doit le déclarer expressément au débiteur (conformément au principe de reconnaissabilité de l'art. 4 al. 4 LPD). Etant donné le fait que le débiteur est tenu de fournir la contre-valeur due, la cession de créance est considérée comme en relation directe avec la conclusion ou la mise en œuvre d'un contrat.

1.9.4 Révision totale de l'ordonnance relative à la nouvelle loi régissant la taxe sur la valeur ajoutée

L'ordonnance relative à la nouvelle loi régissant la taxe sur la valeur ajoutée (OTVA) prévoit la communication de données par procédure d'appel. Le principe de légalité ainsi que le secret fiscal sont applicables en matière de législation fiscale. Notre remarque concernant la procédure d'appel ainsi que notre proposition de créer une ordonnance séparée sur la protection des données ont été complètement ignorées dans le projet d'OTVA. Il manque donc actuellement une base légale suffisante pour une procédure d'appel.

La nouvelle loi régissant la taxe sur la valeur ajoutée (LTVA) arrêtée par le Parlement le 12 juin 2009 est entrée en vigueur le 1er janvier 2010. Le projet d'ordonnance a été mis en consultation fin septembre 2009.

Nous avions déjà pu prendre position lors de la première consultation interne des offices, à la fin du mois d'août 2009. A cette occasion, nous avions constaté une violation du principe de légalité et critiqué alors le fait que ni la LTVA, ni l'ordonnance ne présentaient une base légale suffisante pour la procédure d'appel; nous avions aussi souligné que la procédure d'appel ne pouvait en aucun cas être réglée dans une ordonnance de département. Une subdélégation de ce type est en nette contradiction avec le principe de légalité ancré à l'art. 19 al. 3 LPD. Elle est de ce fait anticonstitutionnelle.

Nous avons recommandé de réglementer de manière suffisamment précise, au moins dans l'ordonnance, le traitement des données, la communication des données et la procédure d'appel. En outre, nous avons proposé, afin de ne pas compromettre l'entrée en vigueur prévue de l'ordonnance, de réglementer dans une ordonnance séparée et de préciser dans une annexe les détails du traitement des données, et tout particulièrement la procédure d'appel (comme le fait l'ordonnance sur le traitement des données de l'administration fédérale des douanes). Ce mode de faire permettrait d'une part de ne pas repousser l'entrée en vigueur prévue de l'ordonnance sur la TVA, d'autre part de laisser suffisamment de temps pour élaborer les normes nécessaires du point de vue du droit de la protection des données.

Au cours de la seconde consultation des offices, nos objections ainsi que notre proposition de créer une ordonnance séparée à propos de la protection des données ont été ignorées. Ni la loi, ni l'ordonnance ne disent quels systèmes d'information il y a, combien ils sont, quelles données ils contiennent exactement, quel but ils servent, la personne précise qui en est responsable et qui a accès à quelles données et systèmes d'information. Selon la volonté du législateur, le principe de légalité doit contribuer à ce que le citoyen puisse régler sa conduite en fonction de la loi et prévoir les suites de son comportement avec un degré de certitude correspondant aux circonstances. En outre, depuis la révision de la LPD en 2008 et l'introduction du principe de la reconnaissabilité à l'art. 4 al. 4 LPD, l'exigence de la transparence revêt une importance plus grande.

Nous avons maintenu notre position en ce qui concerne la procédure d'appel. Il est étonnant que le Département fédéral des finances (DFF) soumette maintenant au Conseil fédéral une ordonnance dont les normes en matière de protection des données sont anticonstitutionnelles. Elles lèsent le principe général de la reconnaissabilité, ce qui implique une atteinte illicite à la personnalité. Nous comprenons d'autant moins cette absence de volonté de coopérer avec le PFPDT que le secret fiscal est inscrit dans la législation fiscale et que l'administration fiscale elle-même devrait avoir un

intérêt fondamental à mettre en place des normes conformes aux règles de protection des données, notamment pour ce qui est de la communication de données.

Les autres suggestions ont été en général prises en considération. Il convient encore de souligner et de notre point de vue de se féliciter de la proposition visant à mettre en place un conseiller à la protection des données en matière de taxe sur la valeur ajoutée.

1.9.5 Proportionnalité des traitements de données concernant la solvabilité

Les agences de renseignements puisent des informations relevant du droit de la poursuite dans les extraits du registre des poursuites. Bien que la loi fédérale sur la poursuite pour dette et la faillite (LP) n'établisse pas de devoirs à l'égard des destinataires de données, les données extraites de registres publics ne peuvent pas être traitées indéfiniment dans des registres privés, pour être ensuite transmises. Nous avons soumis à un expert externe la question de la proportionnalité de la durée du traitement de données par les agences d'informations sur la solvabilité. Cet expert a examiné la question de la proportionnalité en regard du droit de la protection des données et a conclu que la LP posait des limites claires à la durée du traitement de données relevant du droit de la poursuite.

Les agences d'informations sur la solvabilité obtiennent des informations relevant du droit de la poursuite en consultant les extraits des registres des poursuites tenus par les offices cantonaux conformément à l'art. 8a de la loi fédérale sur la poursuite pour dettes et la faillite (LP). Les limites auxquelles ces offices doivent se conformer sont précisées aux art. 8a et 149a LP.

Le traitement de données relevant du droit de la poursuite dans les registres privés des agences d'informations sur la solvabilité occupe aujourd'hui une place de plus en plus grande dans la vie économique. En effet, de nombreux partenaires contractuels, plutôt que de se fonder sur un extrait actuel du registre des poursuites, consultent les fichiers privés d'agences de renseignements. Nous avons voulu soumettre à un expert la question de la proportionnalité du traitement de données relevant du droit de la poursuite par des entités privées de traitement de données telles que les agences de renseignements. L'expert a examiné et évalué la proportionnalité du traitement de données relatives à la solvabilité sur la base de la pratique d'une agence s'étant déclarée prête à coopérer.

L'expert a estimé que le traitement de données effectué par l'agence en question était proportionné et a recommandé à l'entreprise soit d'effacer les évaluations, soit de leur donner la valeur 0 lorsque des faits ne doivent pas être communiqués conformément à l'art. 8a al. 3 LP ou doivent être radiés conformément à l'art. 149a al. 3 LP. L'agence de renseignements a accepté la recommandation et entend la mettre en œuvre.

Au cours de ses recherches, l'expert mandaté a constaté que la communication de données à des tiers par les offices cantonaux de poursuite ne suivait pas de règles uniformes et que des données étaient indûment communiquées à des tiers. Il nous a été conseillé d'inciter les différents offices cantonaux à appliquer la LP de manière uniforme et l'organe fédéral compétent à pratiquer une surveillance accrue.

L'expert a mentionné en outre que l'exécution insatisfaisante des prescriptions de la LP ne pouvait être imputée aux destinataires des données, à savoir les agences de renseignements, car la LP ne prévoit à leur propos aucune obligation. Cela ne signifie pas pour autant qu'elles peuvent traiter des données relevant du droit de la poursuite aussi longtemps que bon leur semble. Il estime que la LP pose des limites claires à la communication de données et qu'elle donne des repères en ce qui concerne le contrôle de la proportionnalité du traitement des données selon la LPD.

Nous avons donc tout d'abord informé le service chargé de la haute surveillance en matière de LP et de faillite, qui fait partie de l'Office fédéral de la justice (OFJ), des résultats de l'expertise. Comme nous l'avions déjà fait dans le cadre des consultations des offices au sujet de la révision de la LP (voir notre 16e rapport d'activités 2008/2009, ch. 1.8.1), nous avons une fois de plus souligné que la communication de données relatives aux poursuites par des agences de renseignements à des tiers prend une place de plus en plus grande dans la vie économique. Du fait que ces données sont de plus en plus demandées par des particuliers, il y a un rapport étroit entre leur traitement étatique par les offices cantonaux des poursuites, leur transmission à des particuliers et leur traitement, relevant du droit privé, par les agences de renseignements.

Les conditions-cadres légales et l'exécution de la LP influencent considérablement l'exercice de l'activité de surveillance du préposé fédéral sur les agences de renseignements. Nous avons donc prié le service de haute surveillance de prendre les mesures qui s'imposent pour que les offices cantonaux des poursuites appliquent correctement la LP et, en cas de transmission de données relative à une poursuite à des tiers, non seulement utilisent une terminologie uniforme, mais aussi suivent une pratique uniforme. On réduit également ainsi les procédures de rectification onéreuses des particuliers désirant faire corriger leurs données auprès des différentes agences de renseignements.

Par ailleurs, nous avons envoyé une circulaire aux agences de renseignements pour les informer des résultats de l'expertise et de notre lettre à la haute autorité de surveillance. Nous leur avons aussi précisé qu'en ce qui concerne la proportionnalité de la durée du traitement des données relatives au droit de la poursuite, nous nous baserons sur les limites légales posées par la LP. Nous avons enfin demandé aux agences de renseignements de nous informer si, à cet égard, le traitement des données qu'elles effectuaient correspondait à nos directives. Les réactions à notre circulaire ont été très diverses. Le PFPDT examine actuellement la suite à donner à cette affaire.

1.10 International

1.10.1 Coopération internationale

L'effectivité de la protection des données passe aussi par la coopération des autorités de protection des données au niveau international et par le développement de normes internationales. Il faut en effet pouvoir donner des réponses concertées aux traitements de données transnationaux auxquels nous sommes de plus en plus confrontés et garantir aux individus les mêmes droits indépendamment de leur lieu de domicile. Dans cette optique, le préposé fédéral participe aux travaux du Conseil de l'Europe, de la Conférence européenne et de la Conférence internationale des commissaires à la protection des données, des instances de contrôle communes Schengen et Eurodac et de l'Association francophone des autorités de protection des données.

Conseil de l'Europe

Nous avons activement participé aux travaux du comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) (Convention 108) et de son bureau. Le comité consultatif a examiné en première lecture le projet de recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Cette recommandation a pour objectif de définir un cadre juridique adéquat et cohérent assurant un équilibre entre la protection des données et les intérêts légitimes pouvant justifier des activités de profilage des individus.

Le T-PD a également adopté son programme de travail pour les prochaines années. Il envisage en particulier d'examiner l'opportunité de compléter la Convention 108 notamment pour répondre aux défis posés par les développements technologiques liés à l'Internet et pour améliorer les mécanismes de mise en œuvre de la Convention. Il pourrait également préparer un instrument juridique contraignant dans le domaine de la coopération policière et judiciaire en matière pénale.

Conférence européenne des commissaires à la protection des données

La conférence annuelle des commissaires européens à la protection des données, qui réunit les autorités de protection des données des Etats membres de l'Union européenne et du Conseil de l'Europe, ainsi que le contrôleur européen à la protection des données et les autorités de contrôle communes dans le domaine de la police et de la justice s'est déroulée à Edimbourg à l'invitation du commissaire britannique à l'information. Sous le thème «améliorer la protection des données en tenant compte des avantages et des faiblesses de la législation européenne en matière de protection des données», les autorités présentes à la conférence ont débattu de l'opportunité de modifier les textes existants et notamment la directive européenne. Elles parviennent à la conclusion qu'il est nécessaire de mettre l'accent sur l'amélioration de l'application des dispositions en vigueur.

La Conférence a adopté une déclaration soulignant le rôle que l'Europe doit continuer à jouer dans la promotion de la protection des données au niveau mondial et rappelant l'engagement des autorités de protection des données pour contribuer au développement d'un niveau élevé de protection. Elle a également adopté une résolution appelant les Etats européens à garantir le respect du niveau de protection des données lors de l'échange de données avec des Etats tiers, notamment en incluant dans les accords internationaux des garanties suffisantes. La Conférence a chargé le groupe de travail justice et police d'élaborer une norme modèle de protection des données.

Groupe de coordination du contrôle Eurodac

Le groupe de coordination du contrôle Eurodac, qui réunit le contrôleur européen à la protection des données et les autorités nationales de protection des données, a terminé sa deuxième inspection conjointe de la base de données Eurodac. Celle-ci contient les empreintes digitales des demandeurs d'asile pour faciliter la procédure d'asile dans l'Union européenne, les pays de l'espace économique européen et la Suisse. L'inspection portait sur le droit à l'information des personnes concernées et sur les méthodes visant à évaluer l'âge des jeunes demandeurs d'asile en vue de leur enregistrement dans la base de données. Le rapport publié sur le site www.edps.europa.eu, sous la rubrique Supervision – Eurodac présente les résultats de l'inspection. Le groupe de coordination adresse des recommandations aux Etats membres et aux autorités européennes. Il estime en particulier que les informations fournies aux demandeurs d'asile sur leurs droits et l'utilisation de leurs données sont relativement incomplètes.

La qualité des informations fournies diffère d'un Etat à l'autre. En outre, les demandeurs d'asile sont en général mieux informés que les immigrés illégaux. Le groupe recommande dès lors d'améliorer la qualité des informations fournies et la manière dont l'information est donnée. Les autorités de protection des données doivent veiller à instruire les autorités compétentes pour que le devoir d'information soit respecté. En ce qui concerne l'évaluation de l'âge des jeunes demandeurs d'asile, les autorités compétentes sont souvent confrontées à des difficultés pour déterminer l'âge d'un enfant. Selon le règlement Eurodac, les empreintes digitales des demandeurs d'asile doivent être relevées à partir de l'âge de 14 ans. Les méthodes utilisées pour évaluer l'âge ne sont pas suffisamment harmonisées, transparentes et fiables. Il conviendrait d'entreprendre une évaluation globale de la fiabilité des différentes méthodes utilisées. Le groupe recommande également d'élever l'âge de la prise d'empreintes à 18 ans.

Le groupe de coordination a entrepris une troisième inspection qui porte sur le système sécurisé pour l'échange d'informations Dublinet, dont les résultats seront publiés en 2010.

Autorité de contrôle commune Schengen

L'autorité de contrôle commune Schengen (ACC) est composée de deux représentants des autorités nationales de protection des données des Etats parties à la Convention d'application des accords de Schengen. La Suisse y est représentée par le PFPDT et par les autorités cantonales de protection des données. L'ACC concentre son activité sur l'interprétation correcte de la convention de Schengen. Sur la base d'inspections coordonnées, elle vérifie si les Etats Schengen respectent les dispositions applicables en matière de protection des données. L'ACC est également appelée à se prononcer sur les développements intervenant dans le domaine du contrôle de l'immigration et de la lutte contre les formes de criminalité. Elle est également appelée à traiter de plaintes déposées par des particuliers. L'ACC a publié son 8e rapport d'activité portant sur la période décembre 2005 à décembre 2008 (voir notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Schengen/Dublin).

L'ACC a achevé deux inspections portant sur l'application de l'article 97 de la convention de Schengen (signalement sur des personnes disparues et sur des personnes devant être placées en sécurité, dans l'intérêt de leur propre protection ou pour la prévention de menaces,) et de l'article 98 (traitement des données des témoins ou des personnes citées à comparaître devant les autorités judiciaires dans le cadre d'une

procédure pénale). Les rapports et les recommandations résultant de ces inspections ont été publiés (voir notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Schengen/Dublin). Les recommandations adressées aux Etats Schengen visent à améliorer la procédure de signalement. L'ACC recommande notamment:

- de mettre en place dans les Etats Schengen des procédures écrites et formelles destinées aux autorités jouant un rôle dans l'introduction de signalements;
- d'assurer la cohérence et l'application de manière uniforme de la procédure lorsque plusieurs autorités procèdent à l'introduction de signalements;
- de soumettre la communication de données relatives à une personne faisant l'objet d'un signalement au sens de l'art. 97 à son consentement écrit ou que ce dernier repose au moins sur une preuve écrite;
- d'assurer que le refus de consentement soit exprimé par écrit ou officiellement enregistré;
- de contrôler à l'aide de moyens automatiques et de procédures formelles les données relatives aux mineurs afin d'empêcher que ceux-ci ne continuent à faire l'objet d'un signalement lorsqu'ils ont atteint l'âge de la majorité;
- d'améliorer le respect des dispositions concernant la réévaluation et les périodes de conservation (art. 98);
- de vérifier que les autorités nationales ayant accès aux signalements y sont bien habilitées.

L'ACC a également mis à jour un guide sur les droits des personnes concernées qui sera publié prochainement.

D'autres textes sur le thème Schengen se trouvent au chiffre 1.4.

Conférence internationale des commissaires à la protection de données

La 31e Conférence internationale des commissaires à la protection des données et à la vie privée s'est déroulée à Madrid du 3 au 5 novembre 2009 à l'invitation de l'agence espagnole de la protection des données (www.privacyconference2009.org). Quelques 1500 participants provenant du monde entier et issus des autorités de protection des

données, des organisations internationales, de différents secteurs de l'économie et du monde académique et scientifique ont participé aux travaux.

La Conférence permet d'aborder avec les autorités compétentes des cinq continents des questions d'intérêt commun et d'actualité ou encore des questions liées aux modalités de coopération. La Conférence s'est intéressée aux défis actuels pour la protection des données que sont les politiques de sécurité, les réseaux sociaux et les technologies d'information et de communications dans un monde interconnecté et globalisé. Les autorités de protection des données, les représentants de la société civile, de l'économie et de l'industrie sont d'accord sur la nécessité de mettre en place un cadre harmonisé pour la protection des données sans considération de frontières.

Ainsi, les commissaires à la protection des données et à la vie privée de quelque 50 Etats ont adopté, à l'unanimité, une résolution saluant un projet de normes internationales pour la protection des données et de la vie privée à la préparation duquel nous avons apporté une contribution active (voir notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – coopération internationale).

Ce projet est une étape importante de la concrétisation des objectifs de la déclaration de Montreux adoptée lors de la 27e conférence internationale en septembre 2005, notamment celui de l'adoption d'un instrument juridique universel contraignant. Il contribue à dégager un dénominateur commun entre les différentes approches de la protection des données et de la vie privée. Il énonce les principes de base de la protection des données communs aux différentes régions du monde et aux différents systèmes juridiques. Il définit les droits des personnes concernées. Il met également l'accent sur la mise en œuvre des exigences de la protection des données, et encourage notamment les mesures proactives et la mise en place d'autorités de surveillance impartiales et indépendantes dotées notamment des compétences suffisantes, de pouvoirs d'intervention et d'investigation et de ressources adéquates. Il revient maintenant aux gouvernements et aux organisations internationales d'asseoir et de concrétiser dans un instrument juridique les principes énoncés dans le projet de normes internationales. Ce dernier constitue également un texte de référence pour les Etats qui entament leur processus législatif dans le domaine de la protection des données.

Le Conférence internationale va poursuivre ses travaux en vue de finaliser un tel instrument. Dans cette optique, nous estimons urgent de soutenir encore plus activement la promotion de la Convention du Conseil de l'Europe et de son protocole additionnel et d'inviter des Etats non membres du Conseil à adhérer à ces deux instruments.

La Conférence a également adopté à l'unanimité une résolution que nous avons présentée et qui tend au renforcement de la coopération internationale au niveau mondial en matière de protection des données et de la vie privée (voir annexe, ch. 4.1.9).

Il s'agit en particulier de renforcer la coopération entre les autorités de protection des données qui sont les indispensables régulateurs au regard des évolutions technologiques qui ne connaissent pas de frontières. Le défi auquel sont confrontées les autorités de protection des données est double. Elles doivent d'abord veiller à ne pas affaiblir le niveau de protection des données existant dans les Etats dotés d'une législation en la matière. Elles doivent ensuite contribuer à amener l'ensemble des pays du monde à reconnaître et appliquer ce niveau de protection pour garantir à tous les individus les mêmes droits en matière de traitement des données personnelles.

La globalisation des échanges, le développement des technologies de l'information et des communications ou la mise en ligne de services de portée mondiale, comme les différents services de Google ou les réseaux sociaux, ou encore l'émergence d'une société de surveillance et le développement des systèmes d'information qui l'accompagne, nécessitent des réponses et des solutions coordonnées et uniformes déterminant les conditions à respecter du point de vue de la protection des données et du droit au respect de la vie privée. Pour atteindre ces objectifs, la Conférence va revoir ses structures et son fonctionnement. Elle pourrait se doter d'un secrétariat permanent.

Association francophone des autorités de protection des données

Nous sommes également actifs au sein de l'Association francophone des autorités de protection des données (AFAPDP), dont nous assurons l'une des 3 vice-présidences. L'AFAPDP a tenu sa 3e assemblée générale à Madrid en marge de la 31e conférence internationale. Cette assemblée a été précédée d'une conférence francophone et d'une rencontre avec le réseau ibéro américain des autorités de protection des données.

Ces deux réseaux ont adopté une déclaration conjointe exprimant notamment leur volonté de contribuer activement au renforcement de la coopération internationale dans le domaine de la protection des données. Ils soutiennent en outre le développement d'instruments internationaux permettant la réduction des divergences existantes parmi les différentes structures légales nationales et régionales sur la protection des données et garantissant au niveau mondial un haut niveau de protection, tout en contribuant à éliminer les obstacles à des échanges d'informations fluides et sûrs au

niveau international. Les deux réseaux vont poursuivre et développer leurs collaborations à l'avenir.

La conférence francophone a mis l'accent sur les défis de la mondialisation des traitements de données personnelles pour les libertés et les droits fondamentaux. On y a relevé l'importance d'un cadre législatif robuste et de la mise en place d'autorités de surveillance indépendantes et effectives. La Conférence a souligné l'intérêt de plus en plus marqué des Etats émergents à se doter d'un régime légal de protection des données et salué la constitution de nouvelles autorités de protection des données, notamment en Tunisie et au Maroc.

La Conférence a également abordé la question cruciale de la protection des données des enfants, notamment à l'ère de l'Internet et des réseaux sociaux. Il a été relevé que les autorités de protection des données ne s'engagent pas suffisamment pour la protection des droits des enfants qui constituent l'un des maillons faibles de la société de l'information. L'AFAPDP, en collaboration avec l'Organisation internationale de la francophonie, va ainsi poursuivre ses efforts en vue de promouvoir la protection des enfants lors du traitement des données les concernant. Elle préparera des instruments de formation et de sensibilisation. Elle va également poursuivre ses efforts pour développer des instruments juridiques contraignants et pour soutenir les nouveaux Etats dans la mise en place de leur législation et de leurs autorités de protection des données.

2. Loi sur la transparence: bilan de l'année 2009

2.1 Demandes d'accès

2.1.1 Départements et offices fédéraux

Le nombre des demandes d'accès déposées est pratiquement identique à celui de l'année précédente. Considéré sur plusieurs années, le pourcentage des accès entièrement refusés est en diminution constante. Par contre, au cours de l'année écoulée, davantage d'accès partiels ont été accordés et les demandes de médiation déposées sont en nette augmentation.

Selon les chiffres qui nous ont été communiqués, 232 demandes d'accès ont été déposées auprès des autorités fédérales en 2009. Dans 124 cas, les autorités ont accordé un accès complet et dans 40 cas un accès partiel. Dans 68 cas, l'accès aux documents a été refusé. Par rapport à l'année précédente, ces chiffres n'ont pas notablement changé (voir la statistique au chiffre 3.5).

Ces chiffres permettent de tirer une conclusion positive: depuis l'entrée en vigueur de la loi sur la transparence (LTrans), le pourcentage des refus complets est en diminution constante. Il était de 43% en 2006, de 33% en 2007, de 32% en 2008 et de 29% en 2009. En revanche, la proportion des accès partiels accordés est passée de 3% en 2006 à 17% en 2009. Et avec 54%, la part des accès entièrement accordés en 2009 correspond exactement à la moyenne des trois dernières années et demie.

Il convient de souligner une fois encore que ces chiffres n'ont qu'une pertinence limitée. En effet, certaines autorités fédérales reconnaissent ouvertement qu'elles traitent «sans formalité» les demandes émanant du public pour lesquelles l'accès va de soi, et ne les incluent donc pas dans la statistique. En outre, certaines unités administratives ne nous ayant pas encore signalé une seule demande d'accès depuis l'entrée en vigueur de la loi sur la transparence il y a trois ans et demi, il est permis de conclure que bon nombre de demandes ne sont absolument pas reconnues en tant que telles. Ainsi, comme pour les années précédentes, nous estimons que le nombre des demandes adressées à l'administration fédérale et traitées positivement est plus élevé que ce que la statistique révèle.

En ce qui concerne les frais, nous constatons comme l'an passé que les offices fédéraux n'ont en général pas demandé d'émoluments pour le traitement des demandes d'accès. Selon les indications fournies par ces offices, seuls six requérants ont dû s'ac-

quitter d'un émolument. Cela dit, avec 3850 francs, le montant total des émoluments encaissés en 2009 est nettement plus élevé que celui des années précédentes (1280 francs en 2008 et 1730 francs en 2007).

Cette année encore, nous n'avons pas pu obtenir d'informations fiables sur la charge de travail occasionnée par ces demandes dans les offices et départements. Les autorités fédérales ne sont pas tenues de nous communiquer la charge de travail associée à l'appréciation d'une demande d'accès. Les informations qui nous ont été transmises ne sont donc pas vraiment significatives. Selon ces informations, la charge de travail a de nouveau augmenté (273 heures en 2007, 509 heures en 2008, 748 heures en 2009).

Indépendamment des demandes concrètes d'accès, un certain nombre de conseillers à la transparence nous ont informés que la charge de travail occasionnée par l'application de la loi sur la transparence a tendance à augmenter. Soulignons tout particulièrement à ce sujet que la participation à une procédure de conciliation (et éventuellement à une procédure judiciaire) peut s'accompagner d'une très lourde charge de travail pour un office.

Depuis l'an dernier, l'Office fédéral de la communication (OFCOM) publie dans une banque de données sur Internet des décisions fondamentales rendues dans le domaine de la radiodiffusion et des télécommunications. Même s'il ne s'agit pas ici, comme dans le cas de la loi sur la transparence, d'information passive mais d'information active, la banque de données des décisions de l'OFCOM contribue aussi pour une grande part à la transparence dans l'administration, outre bien entendu ses autres objectifs.

2.1.2 Services parlementaires

Selon les renseignements fournis par les Services parlementaires, une seule demande leur a été adressée en 2009 suite à laquelle l'accès a été entièrement accordé.

2.2 Demandes en médiation

En 2009, nous avons reçu en tout 41 demandes en médiation (voir la statistique au chiffre 3.7). L'année précédente, elles étaient au nombre de 25. En tout, 29 demandes en médiation ont pu être menées à terme. Dans neuf cas, une solution consensuelle a pu être trouvée avec les parties impliquées. Dans 18 cas nous avons émis des recommandations, car une solution à l'amiable n'a pu être trouvée ou était d'emblée inenvisageable. Parfois nous avons pu clore plusieurs demandes en médiation avec une seule recommandation. Une demande a été retirée et dans un cas, celle-ci n'a pas été remise dans les délais.

Ces chiffres permettent les conclusions et les remarques suivantes:

- Dans 108 cas, les autorités ont complètement refusé l'accès (68) ou ne l'ont accordé que partiellement (40). Suite à ces refus complets ou partiels, 41 demandes en médiation ont été déposées chez nous. Cela signifie donc que dans 38% des accès entièrement ou partiellement refusés, nous avons par la suite reçu une demande en médiation. L'année passée, ceci était encore le cas pour 25% à peine.
- Dans deux tiers à peine des procédures de médiation menées à terme (médiations et recommandations), nous avons réussi à trouver une solution plus favorable pour le requérant (à savoir une médiation ou un accès plus étendu que celui qui avait à l'origine été accordé par l'office fédéral).

Malheureusement, certains requérants doivent encore attendre trop longtemps que la procédure de médiation soit engagée. Par ailleurs, le fait qu'un grand nombre de demande en médiation ont été déposées durant l'année écoulée a eu des répercussions négatives sur la durée des procédures. A deux reprises, le Tribunal administratif fédéral a fait reproche de déni de justice (retard injustifié) au préposé fédéral (arrêts du 16 avril 2009, A-75/2009 et du 16 décembre 2009, A-6032/2009).

2.3 Procédures de médiation closes

2.3.1 Recommandations

Les recommandations émises au cours de l'année écoulée concernant la loi sur la transparence sont résumées ci-dessous. Ces recommandations peuvent être consultées dans leur version originale sur notre site web www.leprepose.ch sous la rubrique Documentation – principe de la transparence – recommandations. Une recommandation importante est publiée en annexe, au chiffre 4.2.

Recommandation DFJP / Conventions de résiliation des rapports de travail de l'ancien secrétaire général et de l'ancien secrétaire général adjoint (9 février 2009)

Le demandeur a requis auprès du Secrétariat général du Département fédéral de justice et police (DFJP) l'accès aux conventions de résiliation des rapports de travail de l'ancien secrétaire général et de l'ancien secrétaire général adjoint. Le DFJP a refusé l'accès avec l'argument que ce dernier pourrait porter atteinte à la sphère privée des

personnes concernées. Dans sa recommandation, le préposé est arrivé à la conclusion que l'intérêt public à l'accès aux conventions l'emportait sur l'intérêt des deux personnes concernées à préserver leur sphère privée.

Le DFJP n'a pas adopté la recommandation du préposé fédéral et a rendu une décision que le demandeur a attaquée devant le Tribunal administratif fédéral. Celui-ci a qualifié de procédure de corapport la proposition émise par le DFJP à l'intention du Conseil fédéral à propos des conventions de résiliation des rapports de travail. La loi sur la transparence n'établit aucun droit d'accès pour les documents de ce type. Le requérant a fait recours contre ce jugement auprès du Tribunal fédéral.

Recommandation Secrétariat général du DDPS – armasuisse / Rapports Benchmarking, armasuisse, Helvetisierung (19 février 2009)

Le demandeur a requis auprès d'armasuisse, plus précisément du Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports (DDPS), l'accès aux rapports «Benchmarking (Vergleich armasuisse mit ausländischen Beschaffungsstellen)», «Die armasuisse der Zukunft» et «Helvetisierung». Les autorités ont allégué que ces trois rapports n'étaient pas terminés et que l'accès avait été refusé sur la base de divers motifs justifiant une exception.

Le préposé fédéral a établi dans ses conclusions que les trois documents devaient être considérés comme terminés. S'agissant des motifs justifiant une exception, il a précisé que la publication de ces rapports ne pouvait avoir des répercussions négatives que sur les relations de politique étrangère ou sur les relations internationales et que l'accès aux rapports devait par ailleurs tout de même être accordé.

Recommandation ODM / Données brutes anonymisées ZEMIS (5 mars 2009)

Le demandeur a requis auprès de l'Office fédéral des migrations (ODM) une liste de toutes les interdictions d'entrée sur le territoire pour l'année 2007 extraite du Système d'information central sur la migration (SYMIC). L'ODM était d'avis que dans ce cas, la loi sur la transparence n'était pas applicable et, de plus, il mettait en doute le fait que les données personnelles contenues dans le SYMIC constituaient des documents officiels. Le préposé fédéral a reconnu l'applicabilité de la loi sur la transparence et objecté à l'ODM que non seulement des données individuelles, mais aussi l'ensemble de toutes les données d'un système d'information étaient en principe accessibles en tant que documents virtuels.

La recommandation (en version allemande) est publiée à l'annexe, ch. 4.2.1.

Recommandation OFAG / Quantités de lait supplémentaires (30 mars 2009)

Le demandeur a requis la publication de toutes les demandes de quantités de lait supplémentaires autorisées par l'Office fédéral de l'agriculture (OFAG), adressées aux organisations de producteurs (OP) et aux organisations producteurs-utilisateurs (OPU) depuis le 1er mai 2008. L'OFAG a refusé l'accès aux documents en question invoquant la protection de données personnelles. Le préposé fédéral n'a pas été en mesure de se prononcer quant à l'argumentation sur le fond avancée par l'OFAG étant donné que les documents en question faisaient partie, au moment de la procédure de conciliation, d'une autre procédure devant le tribunal administratif fédéral. La loi sur la transparence n'a donc pas trouvé application.

Recommandation AFC / Cockpits et Amtsreportings (3 avril 2009)

Le demandeur a requis auprès de l'Administration fédérale des contributions (AFC) l'accès à certains documents de gestion administrative (désignés par les appellations de «Cockpits» et de «Amtsreporting») portant sur les années 2006 à 2008. L'AFC lui en a refusé l'accès au motif que les rapports en question servaient au contrôle, à la conduite et à la direction des affaires et du service et qu'ils étaient donc destinés à l'usage personnel du directeur. L'AFC concluait que la loi sur la transparence n'était en aucun cas applicable. Le préposé fédéral ne s'est pas rallié à cet avis et a retenu dans sa recommandation que les documents de contrôle et de conduite de la direction d'une autorité fédérale relevaient du principe de la transparence et qu'ils devaient donc en règle générale être accessibles.

L'AFC a rejeté la recommandation du préposé et rendu une décision contre laquelle le demandeur a fait recours devant le Tribunal administratif fédéral. Celui-ci est arrivé à la conclusion que l'accès aux documents dits «Cockpits» devait être garanti sous une forme adéquate après anonymisation des données personnelles et après caviardage de certaines informations, sur la base d'exceptions prévues par la loi sur la transparence et dans le respect du secret fiscal. La recommandation (en version allemande) est publiée à l'annexe, ch. 4.2.2.

Recommandation OFSP / Etudes RoKA, bases de calcul, liste des spécialités, conventions tarifaires (22 avril 2009)

Les demandeurs ont requis auprès de l'Office fédéral de la santé publique (OFSP) l'accès aux différents documents en rapport avec la convention tarifaire RBP III (Rémunération du pharmacien basée sur les prestations entre pharmaSuisse et santésuisse). La

convention tarifaire doit être ratifiée par le Conseil fédéral. Comme le Conseil fédéral est, en tant qu'autorité collégiale, exclu du champ d'application de la loi sur la transparence, l'OFSP a refusé l'accès à tous les documents relatifs aux conventions tarifaires transmis au Conseil fédéral. Le préposé ne peut ce rallier à cette argumentation. Il est certes exact que le Conseil fédéral est, en tant qu'autorité collégiale, exclu du champ d'application de la loi sur la transparence. Cependant, la LTrans s'applique lorsque l'office exécute, pour le Conseil fédéral, les tâches administratives en rapport avec l'approbation de la convention tarifaire. Ainsi, les documents ont été examinés par le préposé et jugés accessibles en raison de leur contenu (informations générales).

Deux recommandations DFF / Documents Rencontre entre un membre du Conseil fédéral et une SA (11 mai 2009 et 23 décembre 2009)

Deux demanderesses ont requis auprès du Secrétariat général du Département fédéral des finances (DFF) l'accès à tous les documents en rapport avec une rencontre entre le représentant d'une société anonyme et le chef du DFF. Le DFF a déclaré qu'un seul document avait été remis au Conseil fédéral dans le cadre de la rencontre. Il refusait d'en permettre l'accès du fait de la présence dans ces documents de secrets d'affaires et de l'obligation faite au Conseil fédéral de garder le secret. Le préposé fédéral a examiné les tableaux de gestion des affaires administratives du DFF qui indiquaient que seul le document en question était mentionné. Le préposé a soutenu le DFF dans son argumentation, tout en recommandant la publication de deux courriels qui avaient pour objet l'audition concernant l'accessibilité du document remis.

Recommandation DFAE / Accord de restitution (15 juin 2009)

La demanderesse a requis auprès du Département fédéral des affaires étrangères (DFAE) l'accès à un document concernant un accord de restitution datant de novembre 2005. Environ dix mois après la prise de position négative de l'autorité, la demanderesse a déposé une demande en médiation auprès du préposé fédéral. Dans sa recommandation, le préposé a constaté que le délai légal pour le dépôt d'une demande en médiation n'avait pas été respecté et a relevé que la loi sur la transparence ne s'appliquait pas aux documents officiels qui avaient été produits avant son entrée en vigueur.

Recommandation DETEC / Documents supplémentaires relatifs au compte de l'Etat (19 juin 2009)

Le demandeur a requis auprès du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) l'accès à des documents supplé-

mentaires au compte de l'Etat 2008. Le DETEC a refusé l'accès à ces documents au motif qu'il les avait établis sur mandat d'une commission parlementaire. Il arguait en outre que la loi sur la transparence n'était pas applicable aux délibérations et aux documents de séances des commissions et des délégations parlementaires. Le préposé fédéral est d'avis que cette argumentation ne vaut que si les documents ont été établis sur la base d'un mandat direct et spécifique d'une commission parlementaire. Si les autorités avaient déjà établi les documents au préalable pour elle-même ou pour des tiers (ce qui était en l'occurrence le cas), la dérogation n'est pas applicable. Pour cette raison, le préposé fédéral a recommandé de remettre les documents demandés.

Le DETEC a accepté la recommandation et a informé le préposé fédéral de la remise des documents au demandeur. La recommandation (en version allemande) est publiée à l'annexe, ch. 4.2.3.

Recommandation OFAC / Safety Case Document (Rapport de sécurité) (3 juillet 2009)

La demanderesse a requis auprès de l'Office fédéral de l'aviation civile (OFAC) l'accès au rapport de sécurité de Skyguide, relatif au système d'atterrissage aux instruments ILS RWY 28 Zurich. L'OFAC a refusé cet accès en arguant que les personnes ne connaissant pas bien la matière pouvaient tirer des conclusions erronées du fait de la complexité des documents et que le contenu touchait en outre au secret d'affaires de Skyguide.

Dans une procédure de recours déjà close, le Tribunal administratif fédéral s'était prononcé sur le droit de consultation des mêmes documents, désormais examinés par le préposé fédéral. Il en avait refusé la consultation en argumentant que d'une manière générale, la sécurité de l'aviation civile était menacée en raison de fausses interprétations et qu'en outre, le secret d'affaires de Skyguide était en jeu. Du fait que le Tribunal administratif fédéral s'était déjà prononcé de manière négative à propos de ces documents, le préposé fédéral était lié par l'appréciation de non-accessibilité de ceux-ci.

Recommandation Suva / Documents de contrôle (14 juillet 2009)

La demanderesse a requis l'accès aux documents que la Suva avait établi en tant qu'organe de contrôle en relation avec la vérification d'une machine. La Suva en a refusé l'accès invoquant son propre devoir de discrétion, l'atteinte à la sphère privée du fournisseur de la machine ainsi que l'impossibilité d'anonymiser les données personnelles concernées. Pour cette raison et en l'absence d'un intérêt public prépondérant, le préposé fédéral a donc recommandé de refuser l'accès à ces documents.

Recommandation OFEV- ARE / Étude comparative des sites d'extraction de roches dures (16 juillet 2009)

Des organisations de protection de la nature et de l'environnement ont demandé l'accès à une étude comparative des sites d'extraction de roches dures. D'entente avec l'Office fédéral du développement territorial (ARE), l'Office fédéral de l'environnement (OFEV) a accordé l'accès uniquement à une version anonymisée de l'étude comparative, mais en a refusé l'accès illimité pour plusieurs raisons, entre autres le secret d'affaires et le secret de fabrication des entreprises mentionnées dans l'étude. Dans sa recommandation, le préposé fédéral a constaté que dans le cas d'espèce, il manquait en particulier un intérêt public prépondérant pour pouvoir communiquer les données des entreprises concernées.

Recommandation Fonds de compensation de l'AVS / Expertises relatives à la valeur commerciale d'un bien immobilier (8 septembre 2009)

Le demandeur désirait accéder à deux rapports d'experts concernant la valeur commerciale d'un bien immobilier qui avait été acquis par le fonds de compensation de l'AVS pour son propre usage. Le Fonds de compensation en a refusé l'accès, invoquant le fait qu'il s'agissait de documents de travail internes. Il estimait en outre que la loi sur la transparence ne lui était pas applicable. La législation applicable ne qualifie pas clairement le Fonds de compensation de l'AVS d'unité de l'administration fédérale. Les organisations et les particuliers extérieurs de l'administration fédérale ne sont soumis à la loi sur la transparence que dans les domaines d'activité dans lesquels ils rendent des arrêtés ou des décisions. Dans ses conclusions, le préposé fédéral a estimé que la loi sur la transparence n'était pas applicable et que le Fonds ne pouvait donc pas être tenu de rendre accessibles les expertises en question. Il a recommandé que pour des raisons de transparence, il serait souhaitable qu'une institution chargée d'une tâche publique si importante soit tenue de mettre ses documents à la disposition du public.

Recommandation OFEN / Petites centrales hydrauliques (15 septembre 2009)

Le demandeur a requis l'accès à une liste des coordonnées des petites centrales hydrauliques. L'Office fédéral de l'énergie (OFEN) a refusé l'accès à ces documents pour des motifs relevant de la protection des données. Ces coordonnées auraient permis de déterminer les promoteurs de projets. Le préposé fédéral a considéré ce refus d'accès comme licite et approprié. En particulier, il n'a pas reconnu d'intérêt public prépondérant à la publication des données personnelles des promoteurs de projets.

Six recommandations DFI, DFJP, DDPS, DFF, DFE, DETEC / Documentation supplémentaire concernant le budget 2010 (2 novembre 2009)

Le demandeur a requis auprès des secrétariats du DFI, du DFJP, du DDPS, du DFF, du DFE et du DETEC l'accès à des documents supplémentaires concernant le budget 2010. Les départements ont ajourné cet accès jusqu'à l'adoption de l'objet par l'Assemblée fédérale. Le préposé fédéral a tout d'abord renvoyé à sa recommandation du 19 juin 2009 relative à la documentation supplémentaire des comptes de l'Etat 2008. Pour ce qui est de la documentation supplémentaire concernant le budget, il a reconnu que sa publication prématurée porterait effectivement une atteinte notable au processus de la libre formation de l'opinion et de la volonté de l'organe législatif compétent. Il a toutefois estimé que la formation de l'opinion et de la volonté ne se déroulait pas au sein de l'Assemblée fédérale, mais dans les commissions des finances des Chambres. Il a de ce fait recommandé que l'accès soit repoussé jusqu'au traitement de l'objet par les commissions financières.

Les départements concernés n'ont pas accepté cette recommandation et ont rendu une décision. Ils ont informé le demandeur que la documentation supplémentaire n'entrait pas dans le domaine d'application de la loi sur la transparence et que la compétence de transmettre la documentation revenait donc aux commissions des finances des Chambres.

2.3.2 Médiations

Nous avons trouvé une solution consensuelle dans les cas suivants:

Médiation DDPS / Militaires contractuels

Le demandeur a requis auprès du DDPS divers documents concernant des militaires contractuels (les militaires contractuels sont des employés en uniforme au service de l'armée suisse; ils exercent une activité limitée dans le temps). Suite à la médiation offerte par le préposé fédéral, tous les documents souhaités entrant dans le champ d'application de la loi sur la transparence ont été remis au demandeur.

Médiation Swissmedic / Documents relatifs à des médicaments (deux demandes en médiation)

Swissmedic a refusé aux demanderesses l'accès à des documents concernant des médicaments, invoquant le fait que la demande portait sur un si grand nombre de documents qu'elle ne pouvait pas être traitée. Au terme de deux audiences de médiation, les parties se sont accordées sur un procédé échelonné dans le temps. Elles

ont en outre fixé le montant des émoluments dus. La réalisation des différentes étapes n'est pas encore terminée.

Médiation OFAG / Quantités de lait supplémentaires

Le demandeur a requis auprès de l'Office fédéral de l'agriculture (OFAG) l'accès à des documents concernant la répartition des quantités de lait supplémentaires. Dans le cadre de la médiation, les parties ont convenu que l'OFAG procéderait à un complément d'études concernant l'accessibilité des documents, les démarches requises par l'anonymisation ainsi que les émoluments probables. En outre, elles se sont entendues sur les informations à masquer sur le formulaire de controlling pour des raisons de protection de données. Ces mesures sont encore en cours de réalisation.

Médiation OFSP / In vitro

Les demandeurs ont requis l'accès aux dossiers de la Commission fédérale des prestations générales et des principes (CFPP) concernant la fertilisation in vitro (FIV) et le transfert d'embryons. Cette demande a eu lieu dans la perspective d'une procédure de recours suite au refus de leur caisse-maladie de prendre en charge une FIV. L'OFSP a refusé l'accès aux documents en invoquant les négociations en cours. Au cours de la procédure de médiation, l'OFAP a retiré ses motifs et allégué que la CFPP n'entrait pas dans le domaine d'application de la loi sur la transparence. L'accord suivant a néanmoins été trouvé au cours des entretiens avec les deux parties: l'OFAP remet aux demandeurs les documents anonymisés qui établissent la position de la CFPP sur le thème mentionné.

Médiation IVI / Documents concernant des virus

Le demandeur a requis de l'Institut de Virologie et d'Immunoprophylaxie (IVI) l'accès à de nombreux documents. Le volume des documents désirés laissant présager un émolument élevé, les autorités en ont informé le demandeur et lui ont donné un délai de dix jours pour maintenir sa demande. A l'expiration de ce délai, le demandeur a déposé une seconde demande d'accès, portant sur un nombre réduit de documents.

Cependant, l'IVI l'a à nouveau informé du fait que les coûts seraient encore probablement élevés. Le demandeur a donc désiré soumettre le montant de ces coûts à l'avis du préposé fédéral. Suite à la médiation mise en place par le préposé fédéral, l'IVI s'est déclaré prêt à permettre un accès gratuit à une grande partie des documents.

Médiation FINMA

Le demandeur s'est adressé au préposé fédéral après le refus de l'Autorité fédérale de surveillance des marchés financiers (FINMA), pour des motifs de protection des données, de lui autoriser l'accès à des relevés concernant des intermédiaires d'assurances. Les documents provenaient encore de l'ancien Office fédéral des assurances privées, transféré en 2009 au sein de la FINMA. Après l'ouverture de la procédure de médiation par le préposé, la FINMA a invité le demandeur à un entretien au cours duquel ce dernier a obtenu les informations souhaitées.

Chancellerie fédérale / Directives sur les affaires du Conseil fédéral (Classeur rouge)

Le demandeur a déposé auprès de la Chancellerie fédérale (ChF) une demande d'accès et requis une copie électronique des Directives sur les affaires du Conseil fédéral. Ces directives, également connues sous le nom de «Classeur rouge», régissent la préparation et le déroulement des affaires au Conseil fédéral. Elles fixent également les procédures à suivre et fournissent des canevas des divers documents pouvant être soumis au Conseil fédéral.

La Chancellerie fédérale estimait que permettre d'accéder à ces documents entraverait la libre formation de l'opinion du Conseil fédéral, ajoutant que ces documents étaient classés «internes» et à ce titre, ne devaient pas être rendus accessibles conformément à l'ordonnance sur la protection des informations. Dans le cadre de la procédure de médiation, la Chancellerie fédérale a reconnu que ces arguments ne tenaient pas face à la loi sur la transparence et s'est en définitive montrée prête à remettre au demandeur la copie électronique en question du Classeur rouge.

Médiation OFSP / Mises en évidence de virus

Le demandeur a déposé une demande en médiation parce que l'OFSP ne lui avait pas confié les documents souhaités sur la mise en évidence de certains virus. Au cours des entretiens, une solution satisfaisante pour le demandeur a été trouvée: d'une part l'Office a fourni un document non remis par erreur, d'autre part il a été expliqué au demandeur que la loi sur la transparence ne permettait pas de requérir de la part d'un office l'établissement d'un document précis.

2.4 Evaluation

Trois ans après son entrée en vigueur, le préposé fédéral a présenté le rapport d'évaluation de la loi sur la transparence. Selon ce rapport, une évolution positive a eu lieu d'une manière générale en faveur d'une plus grande transparence dans l'administration fédérale, même si des signes demeurent dans le sens du maintien du principe traditionnel de la préservation du secret. Sur la base de cette évaluation, le préposé fédéral cite dans son rapport les domaines dans lesquels des mesures sont nécessaires.

Selon la loi sur la transparence, le préposé fédéral est chargé de présenter régulièrement au Conseil fédéral un rapport relatif à l'exécution, à l'efficacité et aux coûts de mise en œuvre de cette même loi. Le rapport d'évaluation, établi par un service externe, a été présenté – avec le rapport d'accompagnement du préposé fédéral – dans les délais fixés au Conseil fédéral, à savoir trois ans à dater de l'entrée en vigueur de la loi sur la transparence. La loi sur la transparence exige que le premier rapport se prononce sur les coûts de mise en oeuvre de la loi.

Rapport d'évaluation de l'IDHEAP

Pour des raisons d'objectivité, le préposé fédéral a confié le mandat d'évaluation à un service externe, l'Institut de hautes études en administration publique (IDHEAP). L'équipe de l'IDHEAP a basé son étude sur l'analyse de documents et sur des interviews qualitatives. Il a consulté un grand nombre de conseillers à la transparence de l'administration fédérale et un groupe d'experts constitué de personnes issues du milieu universitaire, du monde du journalisme, ainsi que de représentants qualifiés des départements.

A la question de savoir quels sont les coûts engendrés par l'introduction de la loi sur la transparence, l'équipe de l'IDHEAP a conclu d'une part que non seulement l'investissement consenti pour la mise en œuvre de la loi, mais aussi les coûts annuels résultant du traitement des demandes restent très modestes.

Selon le rapport d'évaluation, plusieurs éléments tendent cependant à montrer une évolution positive dans le domaine de l'accès aux documents officiels. Ainsi, les personnes interrogées qualifient la loi sur la transparence de globalement positive car elle accroît la sensibilité de l'administration à ses devoirs d'information et apporte plus de clarté quant aux droits et aux obligations en matière de transmission d'informations.

L'attitude proactive de l'administration en matière de politique d'information (en particulier la publication de rapports et de documents sur Internet) est considérée comme un effet direct de l'entrée en vigueur de la loi sur la transparence. Elle contribue à son tour à une administration plus transparente. Face à cette évolution positive, on constate dans certaines unités administratives une tendance au maintien du principe de la préservation du secret. Ainsi, il est parfois demandé à la personne désirant accéder à certains documents de donner son identité et ses motivations, deux requêtes contraires à la loi fédérale sur la transparence.

Le rapport souligne par ailleurs certaines pratiques spécifiques visant à limiter l'accès aux documents. Par exemple un office fédéral a décidé de ne pas créer de formulaire de requête en ligne pour restreindre la transmission de demandes. On a également constaté, sur la base de l'analyse de leur site Internet, que certains offices fédéraux vont jusqu'à présenter des informations contraires à la loi, en laissant entendre que l'accès aux documents est en général payant ou que la demande d'accès doit être envoyée par courrier postal alors que la loi autorise toute forme de demande, orale ou écrite.

Sur la base des résultats de leur évaluation, l'équipe de l'IDHEAP a formulé une série de recommandations en faveur d'une administration fédérale transparente. Les évaluateurs proposent entre autres que l'accent soit mis sur la promotion de la loi auprès de la population et sur la sensibilisation des collaborateurs de l'administration fédérale.

Le rapport d'évaluation de l'IDHEAP peut être consulté dans son intégralité sur notre site www.leprepose.ch, sous la rubrique Documentation – principe de la transparence – évaluation 2009.

Rapport d'accompagnement du préposé fédéral

En complément au rapport d'évaluation, le préposé fédéral a établi un rapport d'accompagnement à l'intention du Conseil fédéral. Au terme de trois ans d'expérience, il conclut que l'introduction du principe de la transparence dans l'administration fédérale a correspondu pour l'essentiel aux attentes formulées par le Conseil fédéral et par le Parlement lors de l'élaboration de la loi. Il souligne en particulier le fait que contrairement aux craintes exprimées avant l'introduction de la loi, l'administration fédérale n'a pas été submergée par un flot de demandes d'accès.

Le préposé fédéral estime par ailleurs que l'exécution de la loi présente encore de nombreuses faiblesses. Il préconise des mesures correctives dans cinq domaines:

- Les délais de traitement de la procédure de médiation doivent être prolongés: Jusqu'ici, la plupart des procédures de médiation n'ont pu être closes dans les trente jours, comme le demande la loi, pour diverses raisons pratiques (complexité des cas, manque de personnel, manque de disponibilité de la part de tous les protagonistes pour organiser des séances dans les plus brefs délais, etc.). Il semble que la situation soit comparable dans d'autres pays, où une part importante des procédures de médiation s'étale sur plusieurs mois ou même plusieurs années (voir le rapport d'évaluation de l'IDHEAP, p. 38).
- Les compétences du préposé fédéral doivent être renforcées en ce qui concerne la procédure de médiation: L'évaluation a montré que l'organisation actuelle des procédures dessert beaucoup trop les requérants, qu'il s'agisse d'intenter une action ou de prendre une décision. Ainsi, l'administration peut tarder à remettre un document au préposé fédéral ou ne pas motiver suffisamment un refus, ce qui lui permet de faire traîner la procédure en longueur.

  Les évaluateurs comme le préposé fédéral estiment de ce fait qu'un renforcement des compétences de ce dernier s'impose; il s'agirait par exemple de lui octroyer un droit de donner des instructions à l'administration ainsi qu'un droit de recours contre les décisions de cette dernière lorsque ces décisions s'éloignent des recommandations du préposé fédéral.
- Le seuil en dessous duquel les émoluments ne sont pas facturés doit être relevé: Au cours des trois premières années, il est rare que des émoluments aient été perçus, entre autres pour des raisons d'efficacité (la facturation des prestations n'a pas dépassé les 3000 francs). Le relèvement du seuil minimal à partir duquel les prestations seraient facturées, par exemple de 100 à 500 francs, irait dans le sens de la simplification et de l'unification des procédures administratives.

Le rapport d'accompagnement du préposé fédéral peut être consulté dans son intégralité sur notre site www.leprepose.ch, sous la rubrique Documentation – principe de la transparence – évaluation 2009.

3. Le PFPDT

3.1 Renouvellement de notre système de gestion des affaires (GEVER)

PFPDT travaille depuis dix ans avec son propre système de gestion des affaires (EDÖB-Office). La confidentialité des données est notamment assurée vis-à-vis de tous les administrateurs internes ou externes de l'application. Ceci répond en tout point aux exigences prévues dans le projet de révision de l'ordonnance concernant la protection des informations de la Confédération. D'ici à l'échéance de la migration vers une des solutions standardisées de la Confédération, nous travaillons activement aux aspects organisationnels et techniques de cet important projet.

Depuis le 1er janvier 2000, nous disposons d'un système hautement confidentiel de gestion des affaires (EDÖB-Office). Le concept repose sur un chiffrement de bout en bout (depuis les clients jusqu'au serveur de base de données et aux serveurs d'impression) des contenus potentiellement sensibles. Cette tâche a été réalisée quasiment sans occasionner ni ralentissement, ni alourdissement des travaux rédactionnels accomplis dans l'environnement bureautique traditionnel, avec en outre une intégration de la messagerie électronique. L'avantage substantiel obtenu réside dans la confidentialité absolue des documents, en particulier vis-à-vis des administrateurs (internes) de l'application et des administrateurs (externes) de la base de données, puisqu'ils ne disposent pas des clés nécessaires au déchiffrement des contenus. Le système de classement et l'interface de versement des dossiers aux archives fédérales peuvent encore être améliorés. C'est une des raisons pour lesquelles nous avons décidé de migrer vers une des solutions standardisées de la Confédération, à savoir Fabasoft ou GEVER-Office. Nos premières évaluations ont cependant vite mis en évidence qu'aucun de ces deux produits n'offre un niveau de confidentialité des données équivalent à celui que nous connaissons depuis dix ans. Nous saluons à cet égard le projet de révision de l'ordonnance concernant la protection des informations de la Confédération (OPrI) qui vise à étendre ses exigences de traitement à tous les systèmes informatiques (y compris GEVER), avec un délai de mise en œuvre d'ici à fin 2013. Sans attendre cette échéance, nous travaillons activement à la migration de EDÖB-Office vers un système de gestion des affaires qui répond aussi bien aux exigences du programme GEVER-Bund qu'à celles de la Loi sur l'organisation du gouvernement et de l'administration (LOGA).

3.2 4e Journée européenne de la protection des données

De nombreux jeunes ont déjà été victimes d'insultes, de calomnies ou de harcèlement sexuel ou psychologique sur Internet. Ces incidents montrent qu'il est très important de ne divulguer ses données personnelles qu'au compte-goutte, notamment sur Internet. Lors de la 4e Journée européenne de la protection des données, nous avons participé à diverses manifestations pour informer les écoliers sur les dangers de la Toile.

L'objectif de la journée européenne de la protection des données de cette année était d'examiner comment les jeunes utilisent les nouveaux médias et de les sensibiliser, de même que leurs parents et les enseignants, à la question de la protection de la sphère privée. En effet, même s'ils font un usage fréquent et intensif des moyens modernes de communication, de nombreux jeunes sont peu conscients des dangers qui se dissimulent sur la Toile et des stratégies que l'on peut adopter pour se protéger. Les adultes, eux, sont parfois complètement dépassés par l'évolution rapide des nouvelles technologies et ne peuvent dès lors accompagner leurs enfants.

C'est pour cette raison que nous avons participé à diverses manifestations, aussi bien en Suisse romande qu'en Suisse alémanique. Plusieurs stations de radio romandes et alémaniques ont consacré une émission au sujet des jeunes et de la protection des données sur Internet, et ont permis aux auditeurs de poser des questions à nos spécialistes.

Dans la ville de Berne, le préposé en personne, Hanspeter Thür, a encouragé les écoliers du gymnase de Kirchenfeld à utiliser Internet et ses nombreuses applications de manière responsable. Toute navigation sur la Toile laisse en effet des traces, volontaires et involontaires, qui peuvent porter atteinte à notre sphère privée. Dès lors, afin d'éviter les mauvaises surprises, Hanspeter Thür a conseillé aux jeunes de faire preuve de vigilance et de bon sens dans leurs explorations du monde en ligne. Ceci implique par exemple que l'on lise les dispositions régissant la protection des données ou que l'on ajuste les paramètres de confidentialité des profils des réseaux sociaux (tels que Facebook ou Myspace).

Nous avons, à l'occasion de la journée de la protection des données, publié sur notre site des informations, destinées tant aux jeunes qu'aux parents et aux enseignants, montrant comment naviguer en sécurité sur la Toile (www.leprepose.ch, Thèmes – Protection des données – Internet). On y trouvera notamment une longue liste de liens renvoyant à des sites suisses et étrangers abordant le thème du comportement des jeunes sur Internet.

3.3 Publications du PFPDT – Nouvelles parutions

Notre site web sert de plateforme pour informer le public de nos activités dans les domaines de la protection des données et du principe de la transparence. Au cours de l'année écoulée, nous y avons publié de nouveaux textes concernant divers thèmes. Parmi les nouvelles publications figurent notamment les explications concernant le conseiller à la protection des données d'une entreprise, le traitement mobile des données et les fusions d'entreprise, mais aussi des informations et des conseils sur les risques auxquels s'exposent les jeunes sur la Toile.

Les enfants et les adolescents sont aujourd'hui très vite familiarisés avec les technologies de communication modernes et explorent celles-ci avec un grand intérêt. Cette évolution en soi très positive présente cependant aussi certains risques au niveau de la protection des données. Beaucoup de jeunes utilisateurs ne sont pas suffisamment conscients du fait qu'il est important d'être prudent avec ses données personnelles afin de protéger sa vie privée.

Quant aux adultes, ils sont parfois complètement dépassés par l'évolution rapide des nouvelles technologies et donc dans l'incapacité d'accompagner leurs enfants. C'est pourquoi nous avons publié sur notre site web www.leprepose.ch des informations, conseils et liens sur les risques en matière de protection des données qu'encourent les jeunes sur Internet. Ces informations se trouvent sous la rubrique Thèmes – protection des données – Internet.

Aujourd'hui, l'informatique et Internet nous offrent de nombreuses possibilités de traiter des données lorsque nous sommes en déplacement, possibilités qui sont certes conviviales et efficaces, mais qui soulèvent des questions en termes de sécurité des données, en particulier en ce qui concerne les informations sensibles. Nous avons publié des explications à ce sujet sur notre site web sous la rubrique Thèmes – protection des données –Internet».

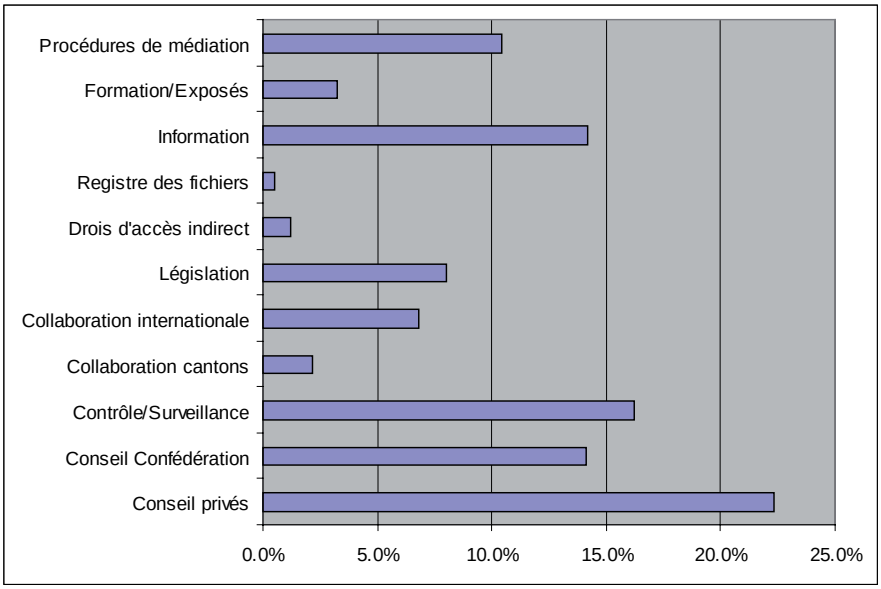
La loi fédérale révisée sur la protection des données du 1er janvier 2008 permet aux entreprises de s'autoréguler. Ainsi, un maître de fichier ne doit pas déclarer ses fichiers s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers. Nous avons maintenant élaboré des explications qui donnent un aperçu des tâches qu'un tel conseiller à la protection des données

doit assumer. Celles-ci se trouvent sous la rubrique Thèmes – Protection des données – Entreprises. Au même endroit se trouvent nos explications sur la transmission de données lors de concentrations d'entreprises, dans lesquelles nous abordons les risques en matière de protection des données qui se présentent lors d'une fusion d'entreprises et où nous décrivons les mesures qui doivent être prises pour garantir la protection des données.

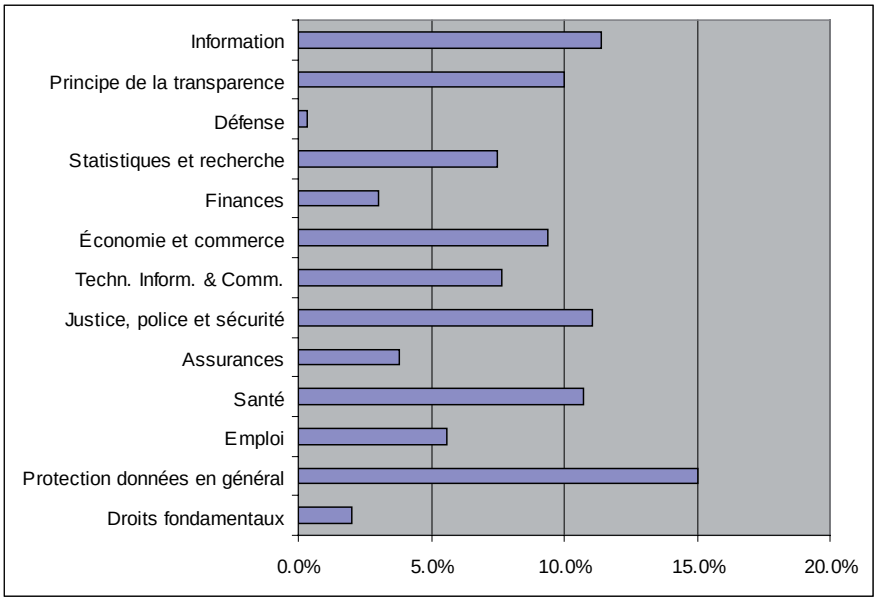
Pour déterminer leur obligation de prise en charge, les assureurs en responsabilité civile demandent régulièrement des expertises sur pièces à des spécialistes externes (médecins, ingénieurs, etc.). Nous expliquons dans notre feuillet thématique quels sont les aspects de la protection des données qui doivent être pris en compte lors de ces expertises. Nous avons également dû aborder le thème de la remise de lettres de sorties et de rapports opératoires aux assureurs-maladie. Le feuillet thématique à ce sujet mentionne les conditions qui doivent être remplies pour qu'un hôpital ou un home puisse communiquer aux assureurs des données personnelles comprises dans ces rapports. Ce feuillet peut être consulté sur notre site www.leprepose.ch, sous la rubrique Documentation – protection des données – feuillets thématiques.

3.4 Statistique des activités du Préposé fédéral à la protection des données et à la transparence (Période du 1er avril 2009 au 31 mars 2010)

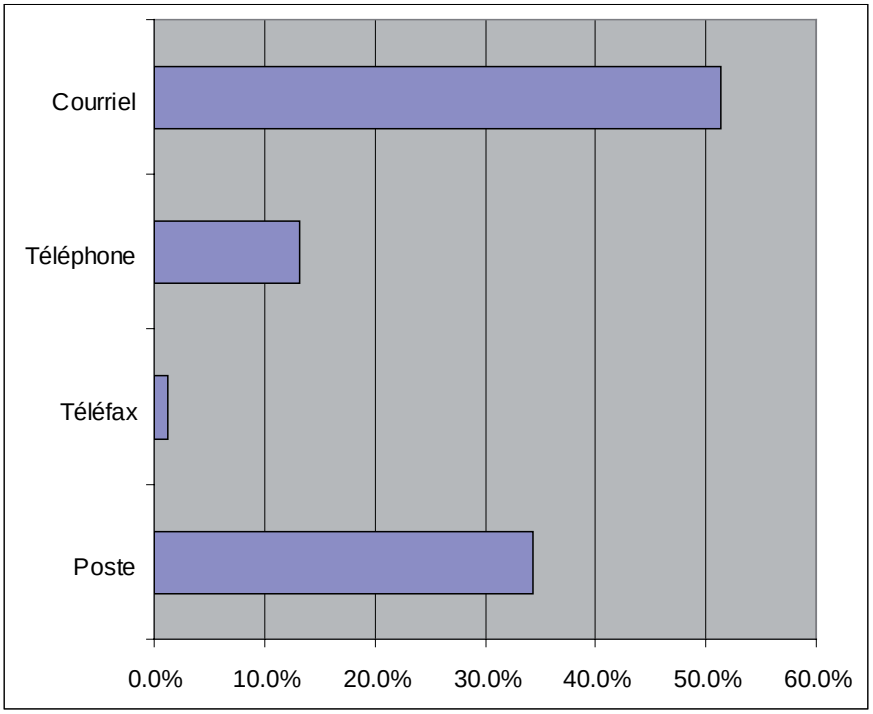
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.5 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2009 au 31 décembre 2009)

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
ChF	27	17	6	4
DFAE	13	7	3	3
DFI	48	22	17	9
DFJP	30	19	8	3
DDPS	20	12	6	2
DFF	11	3	6	2
DFE	28	13	8	7
DETEC	55	31	14	10
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%)
TOTAL 2006 (en %)	95 (100%)	51 (54%)	41 (43%)	3 (3%)

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
ChF	12	6	6	0
PFPDT	15	11	0	4
TOTAL	**27**	**17**	**6**	**4**

Département fédéral des affaires étrangères DFAE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
DFAE	13	7	3	3
TOTAL	**13**	**7**	**3**	**3**

Département fédéral de l'intérieur DFI

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFI	6	2	3	1
BFEG	0	0	0	0
OFC	6	3	3	0
AFS	1	1	0	0
MétéoSuisse	0	0	0	0
OFSP	16	7	4	5
OFS	1	1	0	0
OFAS	9	5	3	1
SER	0	0	0	0
Conseil des EPF	0	0	0	0
SWISSMEDIC	8	3	3	2
FNS	0	0	0	0
SUVA	1	0	1	0
TOTAL	**48**	**22**	**17**	**9**

Département fédéral de justice et police DFJP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFJP	3	1	2	0
OFJ	5	4	1	0
FEDPOL	3	2	0	1
METAS	0	0	0	0
ODM	13	10	2	1
MPC	2	0	1	1
ISDC	0	0	0	0
IPI	1	0	1	0
CFMJ	3	2	1	0
CAF	0	0	0	0
ASR	0	0	0	0
CSI	0	0	0	0
TOTAL	**30**	**19**	**8**	**3**

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

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DDPS / BIG	11	5	4	2
Défense/armée	5	4	1	0
armasuisse	0	0	0	0
OFPP	1	0	1	0
OFSPO	3	3	0	0
TOTAL	**20**	**12**	**6**	**2**

Département fédéral des finances DFF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFF	2	0	2	0
AFF	0	0	0	0
OFPER	1	0	1	0
AFC	7	3	3	1
AFD	0	0	0	0
RFA	0	0	0	0
OFCL	1	0	0	1
OFIT	0	0	0	0
CDF	0	0	0	0
PUBLICA	0	0	0	0
CC	0	0	0	0
TOTAL	**11**	**3**	**6**	**2**

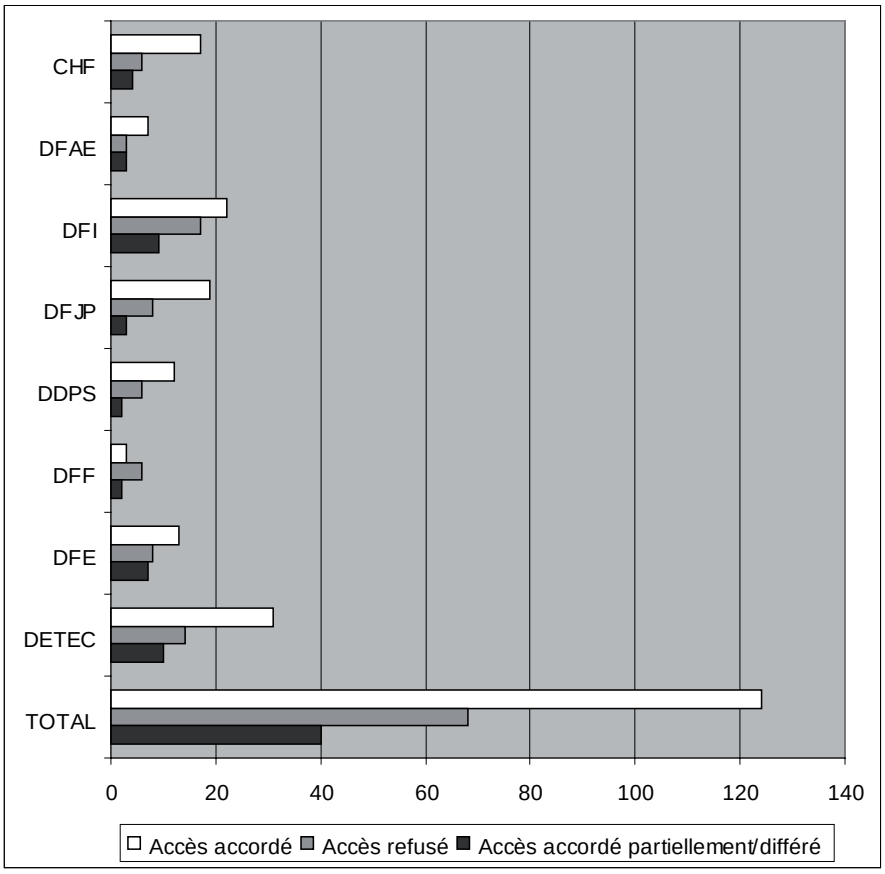
Département fédéral de l'économie DFE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFE	4	0	2	2
SECO	7	4	2	1
OFFT	3	2	1	0
OFAG	5	0	3	2
OVF	6	4	0	2
OFAE	0	0	0	0
OFL	0	0	0	0
SPr	0	0	0	0
COMCO	1	1	0	0
ZIVI	2	2	0	0
BFC	0	0	0	0
TOTAL	**28**	**13**	**8**	**7**

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

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DETEC	1	0	1	0
OFT	5	3	1	1
OFAC	6	5	1	0
OFEN	9	3	5	1
OFROU	1	0	0	1
OFCOM	5	3	1	1
OFEV	17	8	3	6
ARE	0	0	0	0
COMCOM	1	1	0	0
IFSN	3	1	2	0
PostReg	3	3	0	0
AIEP	4	4	0	0
TOTAL	**55**	**31**	**14**	**10**

Traitement des demandes d'accès



3.6 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2009 au 31 décembre 2009)

Services du Parlement SP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SP	1	1	0	0
TOTAL	**1**	**1**	**0**	**0**

3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2009 au 31 décembre 2009)

Catégorie de requérants	2009
Médias	18
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	8
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	7
Entreprises	5
Avocats	2
Universités	1
Total	**41**

3.8 Secrétariat du Préposé fédéral à la protection des données et à la transparence

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

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

Secrétariat:

Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité 1:	8 personnes
Unité 2:	12 personnes
Unité 3:	2 personnes
Chancellerie:	3 personnes

4. Annexes

4.1 Protection des données

4.1.1 Explications concernant le traitement mobile des données

Traitement mobile des données – aperçu

A l'époque où le traitement électronique des données n'existait pas encore, on rédigeait ses textes soit à la main soit à l'aide d'une machine à écrire en prenant soin de garder ceux qui étaient confidentiels dans un meuble que l'on pouvait fermer à clé, à l'abri du regard des curieux. Pour éviter de perdre des documents, notamment dans un incendie, on en faisait des copies, qu'on mettait en lieu sûr.

Aujourd'hui, l'informatique nous offre de nombreuses possibilités de traiter des données, possibilités qui sont certes conviviales et efficaces, mais qui soulèvent des questions en termes de sécurité des données, en particulier en ce qui concerne les informations sensibles. La mobilité de l'homme moderne, notamment, génère de nouveaux risques, qu'il faut prévenir en agissant de manière appropriée. Nous aimerions vous montrer, en prenant l'exemple de Monsieur Remuant, comment procéder concrètement.

Monsieur Remuant se sent bien chez son employeur. Il observe malgré tout attentivement le marché de l'emploi, posant de temps à autre sa candidature aux postes qui éveillent son intérêt. C'est la raison pour laquelle il met à jour son curriculum vitae (CV) à intervalles réguliers.

En homme moderne, adepte de la mobilité, Monsieur Remuant veut pouvoir travailler sur son CV partout et à n'importe quel moment en ayant accès à la dernière version du document. Etant donné qu'un CV contient des informations très personnelles et qu'il constitue, de surcroît, un profil de la personnalité, il est important que sa confidentialité soit garantie en permanence.

Sensibilisé à l'importance de la protection des données, Monsieur Remuant accorde une grande importance à la confidentialité de ses données personnelles. Aussi se demande t il quels sont les critères à remplir pour que le traitement des données soit sûr et respectueux des dispositions régissant la protection des données. Il sait qu'une

enquête réalisée à Londres en 2006 a établi que 55'000 téléphones portables, 5000 assistants personnels, 3000 ordinateurs portables et 900 clés USB ont été retrouvés dans les taxis londoniens en l'espace de six mois[1]. Un autre danger vient des codes malveillants (virus, chevaux de Troie, vers) qui se répandent par le biais des appareils portables. Les cybercriminels ont de plus en plus recours à ce type de procédés pour tenter de mettre la main sur des données personnelles sensibles[2].

Monsieur Remuant vérifie dans quelle mesure le recours aux différentes possibilités dont il dispose lui permet de garantir la confidentialité, l'intégrité et la disponibilité de ses données. Il s'attache en particulier à passer en revue les risques énumérés à l'art. 8 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD):

- destruction accidentelle ou non autorisée;
- perte accidentelle;
- erreurs techniques;
- falsification, vol ou utilisation illicite;
- modification, copie, accès ou autre traitement non autorisés.

De quelles solutions Monsieur Remuant dispose-t-il alors pour le traitement mobile de son CV?

Quatre possibilités (modèles) s'offrent à lui:

- conserver ses données et l'application qui permet de les traiter sur un support local;
- conserver ses données sur un support local et l'application sur Internet;
- conserver ses données sur Internet et l'application sur un support local;
- conserver ses données et l'application sur Internet.

Chacun de ces modèles comporte des exigences spécifiques qui sont importantes pour Monsieur Remuant en fonction de ses attentes en matière de protection des données. Nous allons maintenant les passer en revue.

[1] http://www.pressebox.de/pressemeldungen/ime-mobile-solutions-gmbh-0/boxid-94946.html
[2] http://www.symantec.com/de/de/about/theme.jsp?themeid=smpr_20090415&depthpath=0

Modèle 1: conserver ses données et l'applicationsur un support local

Ce modèle comprend trois variantes intéressantes pour Monsieur Remuant:

a) Les données et l'application se trouvent sur un ordinateur portable ou sur un appareil semblable.

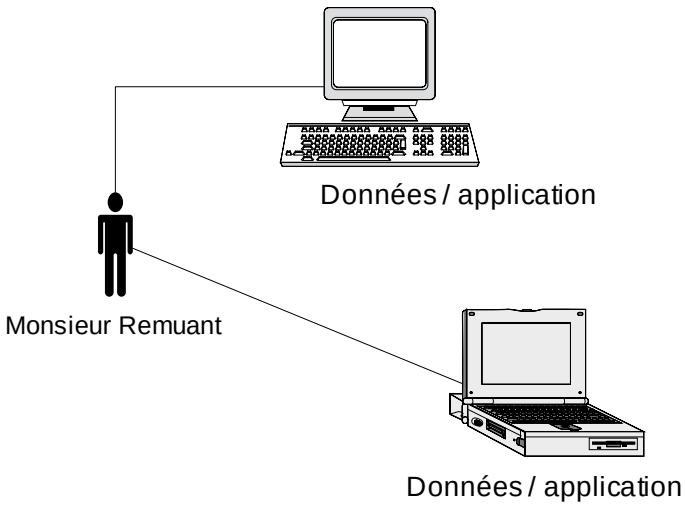
   Monsieur Remuant utilise son ordinateur portable, sur lequel se trouve son CV sous forme électronique et les applications permettant de le traiter. Dans ce cas de figure, il peut traiter les données en question sans support de sauvegarde externe ou portable et sans connexion à Internet.

b) Les données se trouvent sur une clé USB; l'application, sur un PC (p. ex. au domicile de l'utilisateur, sur son lieu de travail ou dans un cybercafé).

   Monsieur Remuant n'a pas d'ordinateur portable. Il conserve son CV sur un support mobile (p. ex. sur une clé USB). Pour pouvoir traiter les données contenues sur ce support, il a besoin d'un ordinateur disposant d'une application compatible. Il peut par exemple relier la clé USB à l'ordinateur qui se trouve à son domicile, sur son lieu de travail ou dans un cybercafé. Il traite les données directement sur la clé. Dans ce cas, il n'a pas besoin non plus de se connecter à Internet, raison pour laquelle il doit absolument copier régulièrement les données sur un appareil sûr (copie de sauvegarde).

c) Les données et l'application se trouvent sur un support mobile.

Caractéristiques et exemples



Une connexion à Internet n'est requise dans aucune des variantes présentées. Tant les données que l'application nécessaire à leur traitement sont sous le contrôle et la responsabilité de Monsieur Remuant dans les variantes a et c.

Exemple

AbiWord[3] est un système de traitement de textes gratuit qui peut être utilisé sur tous les systèmes d'exploitation courants. Il existe aussi en version portable[4] que l'on peut emporter partout sur une clé USB. Ne nécessitant aucune installation, il s'utilise sur l'ordinateur sur lequel on est appelé à travailler, ce qui est très utile si l'ordinateur en question ne dispose d'aucun système de traitement de textes approprié.

Avantages

En conservant les données et l'application sur un support local, on élimine tout risque d'intrusion par des tiers ou d'infection par des maliciels véhiculés par Internet. Par ailleurs, on n'est pas tributaire de fournisseurs de prestations externes. Dans les variantes a et c, la disponibilité des données et de l'application est élevée.

Inconvénients

Monsieur Remuant doit toujours emporter ses supports de sauvegarde (comprenant les données et l'application) en raison du risque de perte ou de détérioration. Qui plus est, il doit faire des copies de sauvegarde, ce qui prend du temps, et sa mobilité est réduite. Dans la variante b, Monsieur Remuant n'a accès à son CV que s'il trouve un PC doté d'une application compatible.

Conclusion: risques et recommandations

Dans le modèle 1, la disponibilité élevée s'obtient au prix de manipulations compliquées. En contrepartie, le degré de confidentialité est élevé.

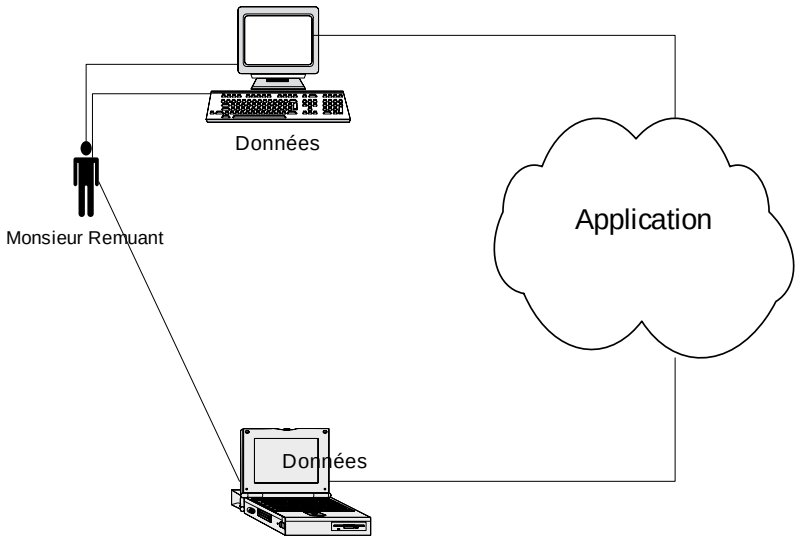
Les données se trouvant sur un support USB risquent d'être perdues, endommagées ou détruites, que ce soit en raison d'un vol ou d'une défectuosité technique. Quiconque utilise des clés USB devrait garder à l'esprit qu'on peut les perdre facilement. C'est la raison pour laquelle il faudrait toujours crypter les données qui sont dignes de protection. Truescript est à cet égard une application simple et gratuite, disponible sur Internet, qui permet de le faire.

[3] http://www.abisource.com/ ou http://abiword.org
[4] http://portableapps.com/

Modèle 2: conserver ses données sur un support local et l'application sur Internet

Ce modèle, où les données se trouvent soit sur un ordinateur (p. ex. un PC ou un ordinateur portable) soit sur un support mobile (p. ex. une clé USB), est plutôt rare. La plupart du temps, les fournisseurs de services Internet mettent à la disposition de l'utilisateur à la fois l'application et la place de stockage pour les données. Pourtant, on peut aussi disposer du même modèle en sauvegardant les données sur un support local et en les effaçant chez le fournisseur de services.

Caractéristiques



Comme Monsieur Remuant n'emporte que son CV avec lui, il doit disposer d'une application d'un fournisseur pour travailler sur son document. Il va la trouver sur Internet. Ce modèle nécessite donc impérativement une connexion à Internet.

Avantages

Monsieur Remuant n'a pas besoin d'emporter l'application avec lui. Ses données seront encore présentes physiquement en cas de défaillance du fournisseur d'accès (p. ex. interruption des prestations). La plupart des fournisseurs de services donnent la possibilité à leurs clients de sauvegarder les données dans des formats courants (pdf, doc, etc.).

Inconvénients

Le traitement des données requiert une connexion à Internet, laquelle peut être une source d'intrusions ou d'infections par des maliciels. Monsieur Remuant est tributaire de la disponibilité de l'application proposée et de sa compatibilité avec les données qu'il possède. Il doit s'attendre à ne plus pouvoir traiter ses données si le fournisseur d'une application propriétaire interrompt ses prestations. Ce genre d'incident ne devrait cependant se produire que rarement.

Conclusion: risques et recommandations

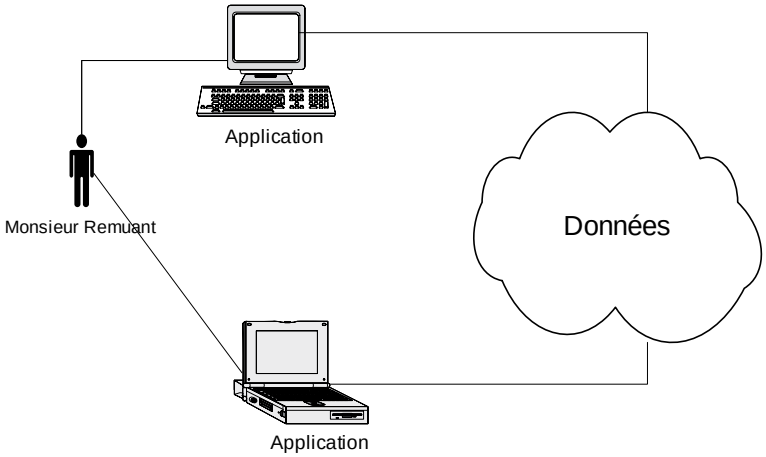
Le risque existe que le fournisseur de l'application fasse des copies des données sur ses serveurs si l'utilisateur les efface après traitement. Il convient de recourir à ce modèle avec précaution si l'on travaille avec des données personnelles sensibles. Il est recommandé de crypter les données avec lesquelles on a travaillé.

Si Monsieur Remuant travaille sur son CV avec l'application Google documents, il peut crypter directement le texte dans le système de traitement de textes (p. ex. avec ClipSecure) et le sauvegarder sous cette forme. Ses données sont dès lors protégées.

Modèle 3: conserver ses données sur Internet et l'application sur un support local

Dans ce modèle, Monsieur Remuant travaille certes sur son CV avec un système de traitement de textes local, mais il confie la sauvegarde de son document à un fournisseur de prestations sur Internet.

Caractéristiques et exemples



Exemple de Wuala[5]

Ce logiciel gratuit basé sur un système pair à pair permet à l'utilisateur de déposer ses documents cryptés sur Internet (l'utilisation de capacités de stockage d'une certaine importance est toutefois payante). La place de stockage sur Wuala se présente comme un disque dur virtuel et doit donc être utilisée comme on le ferait avec un disque réel. Chaque utilisateur peut aussi mettre à disposition une partie de son volume de stockage s'il ne l'utilise pas. Le cryptage et le décryptage s'effectuent sur l'ordinateur de l'utilisateur, si bien que les textes en clair ne quittent jamais l'ordinateur en question. Même les administrateurs de Wuala ne pourraient pas décrypter les documents déposés chez eux.

On peut utiliser par exemple le système de traitement de textes **AbiWord[6]** (voir page 6).

[5] http://www.wuala.com/de/
[6] http://www.abisource.com/ ou http://abiword.org/, http://portableapps.com/

Ce modèle comporte trois variantes intéressantes pour Monsieur Remuant:

a) l'application se trouve sur un ordinateur portable ou un appareil semblable,

b) sur un PC (p. ex. au domicile de l'utilisateur, sur son lieu de travail, dans un cybercafé) ou

c) sur une clé USB.

Avantages

- Qu'il soit à la maison, au bureau, dans un cybercafé ou en déplacement avec un ordinateur portable fonctionnant grâce à un réseau sans fil ou avec un téléphone multimédia, Monsieur Remuant peut accéder à son CV et y travailler. Il n'est pas obligé d'emporter des données sur des supports de stockage.
- Comme il n'emporte pas le fichier contenant son CV, il ne risque pas de le perdre. Il n'a que faire des risques de détérioration des supports de données.
- Monsieur Remuant n'as pas besoin de se soucier de faire une copie de sauvegarde de ses données, car c'est en général son fournisseur d'accès à Internet qui s'en charge. La perte des documents est très improbable.
- En cas de besoin, il est possible de s'adresser à un fournisseur disposant de serveurs se trouvant dans un environnement hautement sécurisé et stockant les données dans un endroit distinct (bunker pour données).
- La plupart du temps, ce service est bon marché.

Inconvénients

- Sans connexion à Internet, Monsieur Remuant peut certes lancer son traitement de textes, mais il ne peut pas accéder à ses documents. L'existence d'un raccordement à Internet est donc une condition sine qua non.

  Monsieur Remuant doit travailler sur un ordinateur équipé d'un traitement de textes (ce qui est le cas, en règle générale) ou emporter un logiciel de traitement de textes avec lui.
- Si le fournisseur d'accès à Internet a la possibilité technique d'accéder aux textes en clair, Monsieur Remuant doit avoir confiance en sa probité.

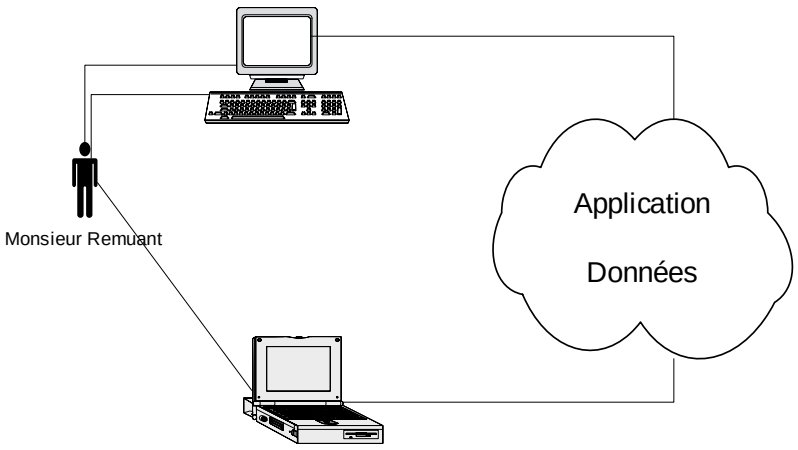
Conclusion: risques et recommandations

- Il faut lire attentivement les conditions générales.
- Il est recommandé de crypter les données déposées chez le fournisseur d'accès à Internet, si possible sur l'ordinateur client.
- Même si le fournisseur d'accès à Internet se soucie de la sécurité et de la disponibilité des documents qui lui sont confiés, il faut en faire des copies de temps en temps et les conserver en lieu sûr.

Modèle 4: conserver ses données et l'application sur Internet

Dans ce modèle, Monsieur Remuant utilise une application se trouvant sur Internet et dépose son CV également sur Internet. Il n'emporte donc avec lui ni application ni données.

Caractéristiques et exemples



Exemple: Google documents[7]

L'application que Google propose gratuitement pour gérer documents et feuilles de calcul fonctionne sur le navigateur Internet de l'utilisateur. Elle ne nécessite l'installa-

[7] http://docs.google.com/

tion d'aucun logiciel supplémentaire. L'utilisateur peut travailler sans problème sur ses textes sur chaque PC raccordé à Internet.

Il est possible de sauvegarder les textes sur un support local et de les télécharger vers le système du fournisseur, mais on n'échappera pas à une sauvegarde automatique régulière sur Internet. Google ne propose pas de cryptage des données. **Zoho Writer[8] et Thinkfree[9],** pour ne prendre que ces deux exemples, sont des applications comparables.

Avantages

- Monsieur Remuant peut s'asseoir devant n'importe quel ordinateur raccordé à Internet (à son domicile, sur son lieu de travail, dans un cybercafé, etc.) et travailler sur son CV. Il ne doit pas emporter de support de données avec lui. Par conséquent, il ne risque pas d'endommager ou de perdre sa clé USB ou un autre support de sauvegarde, voire de se les faire voler. Et même s'il perdait son ordinateur ou s'il se le faisait voler, il resterait en possession de ses données.
- Pendant que Monsieur Remuant travaille sur son document, les modifications qu'il opère sont sauvegardées automatiquement à intervalles réguliers.
- Monsieur Remuant n'a pas à se soucier de faire une copie de sauvegarde.
- Le risque de perdre des données à cause d'un incendie, d'une inondation, d'un vol ou d'un autre événement est faible.

Inconvénients

- Pour pouvoir accéder à ses données et les traiter à sa guise, Monsieur Remuant doit avoir une connexion à Internet qui fonctionne.
- Tant que les données ne sont pas cryptées (Google documents ne propose pas de fonction de cryptage), leur confidentialité est menacée. L'utilisateur n'exerce qu'un contrôle partiel sur ses données.

[8] http://writer.zoho.com/
[9] http://www.thinkfree.com/

Conclusion: risques et recommandations

- Il est recommandé de lire attentivement les conditions générales des fournisseurs de prestations concernés, en particulier les dispositions régissant la protection des données. Il faut savoir avec précision quelles données sont disponibles, qui y a accès et dans quelles circonstances.
- Lors de chaque session de travail, il faut veiller à ne laisser aucune trace ou à faire en sorte que, s'il y en a, elles soient effacées une fois l'application quittée. Ce conseil s'adresse avant tout aux personnes qui travaillent sur un ordinateur qui ne leur appartient pas (p. ex. ceux qu'on trouve dans un cybercafé).
- Il faut choisir de bons mots de passe.
- Il faut utiliser un ordinateur qui ne soit pas infecté par des maliciels afin d'éviter que les documents soient la cible d'attaques. Il faut aussi veiller, côté matériel, à ce qu'aucun enregistreur de frappe ou autre dispositif similaire ne soit installé, qui pourrait intercepter les données saisies par l'utilisateur pour accéder au système test en ligne.
- Il faut aussi choisir un fournisseur d'accès à Internet digne de confiance, qui traite les données personnelles dans les règles de l'art et en toute confidentialité. Un fournisseur d'accès peu scrupuleux pourrait être tenté de vendre les données personnelles qu'il gère s'il était confronté à des difficultés d'ordre économique (p. ex. en cas d'ouverture d'une procédure pour insolvabilité).

Pour crypter des textes, on peut recourir par exemple à **ClipSecure**[10], qui est un gratuiciel facile à utiliser fonctionnant avec toute application basée sur des textes, en particulier avec Google documents, qui fonctionne sur le navigateur Web. Le texte peut être crypté ou décrypté quasiment d'un simple clic de souris. Il convient toutefois de relever que le texte pourrait en principe être consulté pendant qu'on y travaille sur le serveur de Google.

[10] http://www.snapfiles.com/get/clipsecure.html

Réflexion finale

Le choix d'un modèle dépend de plusieurs facteurs, dont certains sont déterminants: les coûts, le caractère digne de protection des données ou les impératifs formels (p. ex. le format du document, le travail en équipe). Par ailleurs, les prescriptions légales et la disponibilité des moyens (p. ex. les accès à Internet) jouent un rôle important. Il est possible d'aménager à plus ou moins grands frais les modèles présentés plus haut pour les rendre conformes aux règles régissant la protection des données.

Aujourd'hui, il est techniquement possible de traiter des données stockées à un endroit différent de celui où l'on se trouve. La qualité d'une telle solution dépend cependant des données à traiter.

Si les données ne contiennent pas d'informations à caractère personnel, aucune des variantes présentées n'est critiquable du point de vue de la législation sur la protection des données. Mais dès qu'on traite, par intérêt personnel ou en vertu d'exigences légales, des données qui ne sont pas destinées à des tiers, des exigences plus sévères s'appliquent aux solutions retenues. Si les informations ne sont pas destinées à un tiers, il faudrait s'en tenir au principe suivant: il faut toujours **crypter** les données, quels que soient l'endroit où elles sont stockées, le support sur lequel elles le sont et l'identité de la personne qui les gère. Ce principe s'applique aussi aux données qui sont conservées sur une clé USB.

La disponibilité des données est un autre facteur entrant en ligne de compte dans le choix d'une solution. Comme nous l'avons mentionné plus haut, les données stockées sont souvent perdues suite à la perte de téléphones mobiles, d'assistants personnels, d'ordinateurs portables ou de clés USB. On a moins de risque de perdre des données si on confie leur stockage et leur gestion à des professionnels de la branche, qui disposent en général de systèmes d'une plus grande stabilité. L'utilisateur doit cependant retenir exactement les données qu'il stocke et l'endroit où il le fait. S'il perd la vue d'ensemble, la réapparition de données dont il n'avait plus souvenir peut lui réserver des surprises.

Il en va de même de la protection des données contre les codes malveillants. Les fournisseurs de prestations professionnels disposent en règle générale de moyens plus efficaces que l'utilisateur final, sur ses appareils portables, pour protéger les données contre les virus, les chevaux de Troie, les vers et les autres logiciels malveillants.

Le tableau ci-dessous indique le modèle à choisir pour minimiser les risques. Il présente, pour chaque modèle, une qualification sommaire des risques énumérés dans l'article 8 ss de l'OLPD. Pour terminer, il convient de relever qu'il n'existe pas de protection absolue pour les données stockées, pas même pour celles qui revêtent un caractère hautement personnel. C'est la raison pour laquelle tout stockage d'une information digne de protection est une opération risquée, quel que soit le système ou le modèle choisi.

Risque / Modèle	Destruction accidentelle ou non autorisée	Perte accidentelle	Erreurs techniques	Falsification, vol ou utilisation illicite	Modification, copie, accès ou autre traitement non autorisés
Modèle 1	faible	élevé	élevé	moyen	faible
Modèle 2	faible	élevé	élevé	moyen	moyen
Modèle 3	faible	faible	moyen	faible/moyen	faible/moyen
Modèle 4	faible	faible	moyen	faible/moyen	moyen

Documents et liens connexes

Praxistipp: Sicherheit von USB-Sticks in Unternehmen. In: Datenschutzberater 4/2009

PC News: «Installationsfreie Programme und USB-Sticks». 2008, in: http://pcnews.at/?Id=14611&Type=Htm

FoeBud e.V.: PrivacyDongle – Anonym im Internet surfen. 2009, in: https://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/privacydongle/index

Pressetext Austria: Datenspeicher der Zukunft sind im Web. 2.10.2008, in: http://pressetext.ch/news/081002003/datenspeicher-der-zukunft-sind-im-web/

Fraunhofer Institut: Privatsphärenschutz in Soziale-Netzwerke-Plattformen. 2008, in: http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf

News.ch: Das Internet als Daten-Tresor oder gemeinsame Festplatte. 13.01.2009, in: http://www.news.ch/Das+Internet+als+Daten+Tresor+oder+gemeinsame+Festplatte/330494/detail.htm

Bildung Schweiz: Büro 2.0 – online sein ist alles. 2009, in:
http://www.lch.ch/dms-static/e08a9090-8a86-4473-a6a0-8e96778395a4/
bildungsnetz 37.pdf

PC-Welt: Kostenloser Datenspeicher im Netz. 2008, in:
http://content8.wuala.com/contents//Wuala/Blogs%20and%20Press/German/Magazine%20-%20Print%20und%20Online/2008-09-24%20PC%20Welt.pdf

Thomas Söbbing: Cloud Computing – die Zukunftsvisionen von Amazon, Google und Microsoft rechtlich betrachtet. 2009, in: jusletter.ch vom 10.8.09.

World Privacy Forum: Privacy in the Clouds – Risks to Privacy and Confidentiality from Cloud Computing. 2009.

Landesbeauftragter für den Datenschutz Niedersachsen: Mobiles Arbeiten – datenschutzgerecht gestaltet, Orientierungshilfe und Checkliste. 2003.

4.1.2 Informations et conseils concernant l'utilisation des moteurs de recherche

Introduction

Les moteurs de recherche sont aujourd'hui indissociables d'Internet, car, sans eux, il serait quasiment impossible de s'y retrouver sur la Toile, avec ses milliards de pages. Ils doivent toutefois recenser de manière ciblée les informations sur le comportement de recherche des internautes et sur la qualité des résultats, mais aussi les évaluer selon des méthodes statistiques, pour faire augmenter sans cesse le taux de réussite des recherches d'informations sur Internet. Rien que la croissance continuelle du nombre de pages Internet oblige les exploitants de moteurs de recherche à traiter un volume d'informations en constante augmentation.

Si les moteurs de recherche apportent leur contribution à la société de l'information ou de la connaissance et, par là même, à la croissance économique durable de notre société, ils **s'immiscent aussi dans la sphère privée des internautes** en traitant des données les concernant, tant lors de l'évaluation des requêtes que lors de la fourniture des résultats des recherches.

Les moteurs de recherche soulèvent des problèmes en termes de protection des données

Le recours à des moteurs de recherche soulève deux grandes problématiques. La première concerne la **collecte d'informations figurant sur des pages Internet distinctes, indépendantes les unes des autres**, que l'affichage des résultats de la recherche rend accessibles à l'internaute. La seconde porte sur le fait que les moteurs de recherche recueillent, moyennant l'enregistrement de l'adresse IP, **toutes les recherches de l'internaute, tous les résultats de ces recherches et toutes les consultations de pages figurant dans les résultats**, et qu'ils peuvent ainsi établir les profils de la personnalité des internautes, les évaluer et les exploiter.

Informations et conseils

- Sitôt que des données sur une personne déterminée sont disponibles sur Internet, il est très facile de les trouver grâce à des moteurs de recherche. Ces derniers permettent aussi de rassembler des informations disséminées. Face à ce constat, les internautes devraient déterminer avec le plus grand soin **quelles informations** les concernant ils veulent faire figurer sur Internet.

- Prises séparément, des données peuvent certes être tout à fait anodines (p. ex. des informations sur l'appartenance à telle ou telle association, sur l'emploi qu'on occupe, sur les études que l'on a faites, etc.). Mais en réunissant et en analysant ces informations, on peut rapidement établir un **profil de la personnalité** en ligne. Dans de nombreux cas, les internautes disent n'avoir jamais eu l'intention de rendre un tel profil accessible sur Internet. A cet égard, il faut relever que les données peuvent être publiées sur Internet **par des tiers**.

- Il est pratiquement impossible d'empêcher des moteurs de recherche de réunir des informations sous la forme de résultats de recherches. C'est aux personnes concernées de s'adresser aux exploitants des sites Web pour faire valoir leurs droits de rectification ou d'effacement des données les concernant. C'est pourquoi les internautes doivent **toujours garder un œil** sur les données les concernant qui sont disponibles sur Internet et qui pourraient être réunies par un moteur de recherche.

- Si vous exploitez un site Web, vous pouvez donner des **instructions** en langage HTML aux moteurs de recherche pour qu'ils n'indexent pas telle ou telle page.

- Si une personne concernée utilise, en plus des fonctions de recherche, **d'autres services offerts par l'exploitant**, notamment des services de messagerie, l'exploitant peut identifier non seulement l'adresse IP, mais aussi la personne à laquelle elle correspond. En **combinant** les données des requêtes **avec les données relatives à l'identité de la personne en question**, il pourrait aussi établir un profil de la personnalité. En admettant que quelqu'un recherche régulièrement des informations sur une maladie bien précise, on pourrait en déduire que cette personne souffre de cette maladie. La diffusion de ces données pourrait porter préjudice à la personne en question.

- Etant donné que les exploitants de moteurs de recherche vivent avant tout de la publicité qu'ils diffusent en ligne, laquelle doit être aussi efficace et **ciblée** que possible, ils ont tout intérêt à combiner les données des requêtes avec les données relatives à l'identité des personnes qui effectuent les recherches. Cette pratique ne pose aucun problème tant que les données en question (profils de la personnalité) ne sont pas utilisées à d'autres fins (p. ex. communication à une compagnie d'assurance en vue du calcul des primes).

- Il convient par ailleurs de relever que presque tous les moteurs de recherche **sauvegardent** l'ensemble des **requêtes**, y compris les adresses IP, pendant une période relativement longue (plusieurs mois en règle générale). Mais il existe aussi des moteurs de recherche qui effacent plus rapidement les données d'identification des internautes, voire qui ne les sauvegardent pas (p. ex *cuil.com ou scroogle.org*).

- Si vous avez recours à des moteurs de recherche, vous ne devez pas oublier que de telles possibilités de **combinaisons** existent, et donc que **vous devez déterminer** de quelles prestations fournies par un exploitant vous voulez bénéficier et combien vous en voulez. Qui plus est, les règles de confidentialité édictées par le fournisseur peuvent donner des indications sur les pays dans lesquels les données sont traitées et sur la durée de leur conservation.

4.1.3 Explications concernant les conseillers à la protection des données en entreprise

Le conseiller à la protection des données dans la loi

De nouvelles dispositions introduites par la loi révisée sur la protection des données du 1er janvier 2008 (LPD RS 235.1) permettent aux entreprises de s'autoréguler. Conformément à l'art. 11a, al. 5, let. e le maître du fichier n'est pas tenu de déclarer son fichier s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers. Le préposé fédéral à la protection des données et à la transparence (ci-après: préposé) doit en être informé.

Dans sa version allemande, la LPD utilise le terme de «Datenschutzverantwortlicher», ce qui signifie «responsable de la protection des données», alors que la version française parle de «conseiller à la protection des données». Etant donné que le législateur n'avait pas l'intention de décharger le maître du fichier de sa responsabilité et de la faire endosser par le conseiller à la protection des données, la LPD doit être interprétée selon la version française. C'est donc avant tout au maître du fichier (ou, plus précisément, à l'entreprise qui traite les données) d'assumer la responsabilité. Le conseiller à la protection des données n'est responsable que dans les limites prévues par l'art. 55 de la loi fédérale complétant le Code civil suisse (Livre Cinquième: Droit des obligations CO, RS 220).

Les tâches et le statut du conseiller à la protection des données en entreprise (ci-après: conseiller à la protection des données) sont régis par les articles 12a et 12b de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD, RS 235.11).

Statut du conseiller à la protection des données en entreprise

Pour être à même d'exercer sa fonction de surveillance, le conseiller à la protection des données doit pouvoir assurer en toute indépendance l'application interne des dispositions relatives à la protection des données (art. 11a, al. 5, let. e, LPD). Afin que l'autorégulation puisse fonctionner efficacement, l'indépendance du conseiller à la protection des données doit être garantie tant du point de vue organisationnel et matériel que du point de vue de l'activité qu'il exerce dans l'entreprise.

Indépendance au plan organisationnel

Afin de pouvoir accomplir ses tâches dans l'entreprise, le conseiller à la protection des données ne doit pas exercer des activités incompatibles avec celles-ci. Son statut à lui seul doit déjà permettre d'éviter tout conflit d'intérêts. Dans la pratique, on constate que les entreprises confient généralement ces tâches à un état-major ou créent un poste à cet effet au service juridique. Il arrive aussi que le conseiller à la protection des données soit rattaché au service informatique ou au comité directeur.

Si l'on veut écarter tout risque de conflit d'intérêts, il faut veiller à ce que le poste de conseiller à la protection des données ne soit pas intégré dans la hiérarchie directe. A cet égard, les entreprises disposent de différentes possibilités allant de la création d'un état-major à la désignation d'un conseiller à la protection des données externe.

Indépendance au plan matériel

Pour être à même d'assumer ses tâches correctement et en toute indépendance, le conseiller à la protection des données doit en outre disposer des compétences requises. Le droit se borne à indiquer qu'il doit avoir les connaissances professionnelles nécessaires (art. 12a, al. 2, et 12b, al. 2, let. a, OLPD) sans pour autant préciser lesquelles.

On exige de lui à la fois des connaissances dans le domaine de la protection de données et des connaissances spécifiques propres à l'entreprise. Il devrait notamment connaître et savoir appliquer les grands principes de la loi sur la protection des données. S'il n'a pas déjà des connaissances juridiques, il faudrait le former de manière à ce qu'il soit au moins en mesure de juger si, quand et dans quelle mesure un traitement de données personnelles est susceptible de porter atteinte à la personnalité d'un individu.

Le préposé recommande donc qu'un conseiller à la protection des données (qui ne bénéficierait pas d'une formation juridique antérieure) ait travaillé au moins six mois dans le domaine de la protection des données ou qu'il reçoive une formation de cette durée.

Le conseiller à la protection des données doit par ailleurs connaître l'entreprise. Il doit notamment pouvoir évaluer, sur la base de ses connaissances spécialisées, les normes techniques appliquées, l'organisation du maître du fichier et les divers traitements de données personnelles du point de vue de la législation sur la protection des données. Selon l'entreprise, cela revient à exiger de lui des compétences techniques très pointues. Ainsi, dans une entreprise du secteur des technologies de l'information et de la communication, il devrait à tout le moins disposer d'une expérience technique

suffisante (p. ex. en qualité de programmeur) pour être à même de superviser les traitements de données tant du point de vue technique que sous l'angle de la protection des données.

Indépendance du conseiller par rapport à ses activités

Le conseiller à la protection des données doit, dans l'exercice de ses fonctions, être suffisamment indépendant pour pouvoir assumer ses tâches sans recevoir d'instructions et sans risquer de se faire sanctionner par l'entreprise à cause de son activité. En outre, il doit disposer des ressources nécessaires (le plus souvent sous forme de temps de travail) à l'accomplissement de ses tâches propres à l'entreprise (art. 12b, al. 2, let. b, OLPD). Les exigences varient certes en fonction de la taille de l'entreprise; le préposé exige cependant que le poste de conseiller à la protection des données soit doté de suffisamment de ressources pour que la fonction soit plus qu'un simple alibi.

Enfin, le conseiller à la protection des données doit avoir accès à tous les fichiers, aux traitements et aux informations nécessaires à l'accomplissement de sa tâche (art. 12b, al. 2, let. c, OLPD), ce qui implique qu'il y ait non seulement accès sur demande, mais qu'il ait aussi connaissance de tous les traitements de données au sein de l'entreprise.

Tâches du conseiller à la protection des données

L'OLPD prévoit essentiellement deux catégories de tâches pour le conseiller à la protection des données:

- contrôler les traitements de données personnelles et proposer des mesures s'il apparaît que des prescriptions sur la protection des données ont été violées (art. 12b, al. 1, let. a, OLPD).
- dresser l'inventaire des fichiers gérés par le maître du fichier mentionné à l'art. 11a, al. 3, LPD (art. 12b, al. 1, let. b, OLPD).

Fonction de surveillance du conseiller à la protection des données

Pour être en mesure d'exercer toutes les tâches qu'implique cette fonction, le conseiller à la protection des données doit connaître tous les fichiers et les traitements de données qui existent dans l'entreprise. Il doit donc avoir, au sein de l'entreprise, le droit de consulter tous les documents requis, de se faire présenter l'ensemble des systèmes de traitement des données et d'obtenir tous les renseignements nécessaires de la part de toutes les personnes responsables du traitement des données. Ceci implique

que le conseiller ait le droit de donner des instructions, et il incombe à l'entreprise de faire en sorte que ces instructions soient respectées.

Le préposé recommande par conséquent d'instaurer un **devoir de déclarer** tous les fichiers et traitements de données au conseiller à la protection des données (cliquer sur le lien ci-après pour consulter le formulaire pour la déclaration de fichiers).

Sur la base des informations qu'il aura obtenues dans le cadre de sa fonction de surveillance, le conseiller à la protection des données devra évaluer si et dans quelle mesure des prescriptions internes et légales concernant la protection des données ont été violées (ou sont susceptibles de l'être). Cette tâche impliquera aussi une analyse des risques (p. ex. risque de transmission, d'effacement ou de traitement non intentionnel ou illicite des données, risque de perte de données ou risque d'une erreur technique, etc.). S'il constate, dans le cadre de ses investigations, que des prescriptions ont été violées, il doit pouvoir recommander des mesures. L'organisation interne de l'entreprise déterminera si ces recommandations doivent être adressées à la direction ou aux collaborateurs compétents. Quel que soit le cas de figure, l'entreprise devra faire en sorte que les recommandations soient mises en œuvre. Si elle ne le fait pas, il y aura lieu de considérer que les prescriptions en matière de protection des données ont été violées intentionnellement. Au cas où l'affaire devrait être rendue publique, l'image de l'entreprise concernée risquerait d'être sérieusement écornée.

Exception à l'obligation de déclarer les fichiers

Conformément à l'art. 11a, al. 5, let. e, LPD, l'entreprise n'est pas tenue de déclarer ses fichiers si elle a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données. Elle doit toutefois être organisée de manière à pouvoir renseigner, sur demande, des personnes privées et le préposé sur les fichiers contenant des données sensibles ou des profils de la personnalité qui sont régulièrement traités ou sur la base desquels des données personnelles sont régulièrement communiquées à des tiers.

Ce sont là les exigences minimales prévues par la LPD pour que le maître du fichier soit délié de l'obligation de déclarer. Dans l'intérêt de l'entreprise, le préposé recommande cependant que le conseiller à la protection des données examine tous les fichiers dont dispose l'entreprise.

Mesures et recommandations

Les mesures prescrites par la loi et régissant l'organisation interne de l'entreprise dans le domaine de la protection des données sont exposées ci-après. Le préposé formule par ailleurs des propositions organisationnelles devant être respectées par toute entreprise soucieuse de répondre aux exigences de la protection des données.

Prescriptions légales

En vertu des prescriptions légales, le conseiller à la protection des données doit remplir les conditions suivantes:

- Il n'est pas soumis aux instructions du maître du fichier.
- Il doit disposer des qualifications professionnelles nécessaires.
- Il doit contrôler les traitements de données personnelles au sein de l'entreprise.
- Il doit pouvoir proposer des mesures s'il apparaît que des prescriptions sur la protection des données ont été violées.
- Il doit avoir accès à tous les fichiers et à tous les traitements de données.
- Il doit dresser l'inventaire des fichiers selon l'art. 11a, al. 5, let. e LPD et le tenir à la disposition du préposé ou des personnes concernées qui en font la demande.
- Il ne doit pas exercer d'activités incompatibles avec ses tâches de conseiller à la protection des données.

Afin que l'entreprise puisse être déliée de l'obligation de déclarer, elle doit répondre aux exigences précitées et informer le préposé qu'elle a désigné un conseiller à la protection des données.

Propositions organisationnelles du préposé

Une entreprise a, dans tous les cas, intérêt à accorder à la protection des données une importance supérieure à celle que prévoit la loi. Vu la sensibilité de la population, toute violation de la loi sur la protection des données est susceptible - si elle est rendue publique - d'avoir un grand retentissement médiatique et donc de nuire considérablement à l'entreprise. Le préposé tient par conséquent à souligner qu'il est dans l'intérêt même de l'entreprise de mettre en place une surveillance interne efficace en matière de protection des données.

Organisation hiérarchique de la protection des données au sein de l'entreprise

L'entreprise devrait non seulement désigner un conseiller à la protection des données indépendant mais aussi mettre en place des responsables de la protection des données aux niveaux hiérarchiques inférieurs (ci-après appelés les coordinateurs de la protection des données), qui consacreront une partie de leur temps de travail à la protection des données dans leur service ou leur secteur. Ils seront chargés d'assurer

la communication entre le conseiller à la protection des données et les différents services ou secteurs afin que d'éventuels problèmes dans les services soient identifiés et signalés à un stade précoce et que les informations et instructions puissent être adressées directement aux services concernés.

Une telle structure peut être utile, à différents points de vue, au conseiller à la protection des données:

1. Instruction des collaborateurs par les coordinateurs de la protection des données (qui ont été formés préalablement par le conseiller);
2. Rencontres entre les coordinateurs de la protection des données des différents services ou secteurs en vue d'un échange d'informations et de connaissances;
3. Discussion, avec un interlocuteur direct, de problèmes concernant un service ou un secteur dans le but de formuler des recommandations ou de donner des instructions;
4. Déclaration de fichiers et de traitements de données au responsable de la protection des données pour transmission au conseiller à la protection des données, le coordinateur exerçant alors une fonction de standardisation et de centralisation;
5. Relais permettant d'avoir connaissance, à un stade précoce, des traitements de données prévus, préparés ou effectués au sein de l'entreprise.

Afin que la communication entre le conseiller à la protection des données et les coordinateurs de la protection des données soit aussi efficace que possible, il est recommandé de ne créer aucun échelon hiérarchique intermédiaire. Si la charge de travail devient trop lourde pour le conseiller à la protection des données, du fait qu'il est sollicité par un trop grand nombre de coordinateurs de la protection des données, le préposé recommande de désigner un deuxième conseiller à la protection des données. Les coordinateurs de la protection des données peuvent alors être répartis entre les deux conseillers, aucun échelon intermédiaire ne devant être créé.

Procédures standardisées

Le préposé recommande aux entreprises de mettre en œuvre quelques procédures spécifiques standardisées que les collaborateurs devraient appliquer au quotidien:

1. *Déclaration et contrôle de fichiers*: Le conseiller à la protection des données devrait si possible avoir connaissance de tous les fichiers dont dispose l'entreprise. Il convient donc de créer et de distribuer dans l'entreprise un

formulaire standardisé recensant tous les fichiers et traitements de données existants ou prévus. Il y aura ainsi moyen de superviser l'ensemble des données, les mutations et l'effacement de fichiers, et le conseiller à la protection des données pourra savoir en tout temps quelles données sont traitées par quel service ou secteur.

2. *Evaluation des risques*: Le conseiller à la protection des données devrait procéder à une analyse des risques sur la base des déclarations et des contrôles de fichiers et de traitements de données. Cette analyse devrait lui permettre d'évaluer le dommage potentiel le plus grave. Pour les fichiers sensibles (risque élevé pour l'image de l'entreprise, préjudice important pour les personnes concernées, dont l'entreprise pourrait être tenue responsable, etc.), le conseiller à la protection des données devrait prévoir non seulement des mesures de sécurité suffisantes mais aussi des scénarios-catastrophe pour parer à toute éventualité.

3. *Communication de violations de la législation sur la protection des données*: Pour limiter au maximum les risques et faciliter la mise en œuvre des scénarios-catastrophe, il est extrêmement important, en cas de violation de la législation sur la protection des données, que les informations circulent rapidement entre le service concerné et le conseiller à la protection des données. C'est d'autant plus vrai lorsque ladite violation risque d'être dévoilée au grand jour au détriment de la crédibilité de l'entreprise. Les coordinateurs de la protection des données doivent donc pouvoir évaluer approximativement la portée d'une violation potentielle et l'urgence de la menace.

Site interne et formulaire standard

En outre, le préposé recommande de créer, sur l'intranet de l'entreprise, un site consacré à la protection des données, sur lequel seront mis à disposition tous les documents et formulaires pertinents. Les collaborateurs auront ainsi la possibilité de s'informer par eux-mêmes.

Les entreprises devraient créer des formulaires standard pour la déclaration de tous les fichiers et traitements de données, lesquels permettront en outre aux conseillers à la protection des données d'avoir connaissance de tous les traitements de données auxquels procède l'entreprise.

4.1.4 Transmission de données lors de concentrations d'entreprises

Les concentrations d'entreprises et l'aliénation de parties d'entreprises sont monnaie courante dans les milieux économiques. Pour notre propos, nous distinguerons ici deux phases: la phase de préparation et de conclusion du contrat d'une part, et la phase de reprise de l'entreprise d'autre part. Au cours de la première phase, les différentes parties (soit les partenaires de la fusion, soit la personne qui aliène et celle qui acquiert l'entreprise ou la partie d'entreprise) mènent des négociations en vue de conclure un contrat de fusion ou de vente. Puis vient la concentration effective des entreprises ou la reprise de la partie d'entreprise par l'acquéreur.

Les entreprises traitent quasiment en permanence des données concernant des personnes et sont donc tenues de respecter les dispositions pertinentes de la loi fédérale sur la protection des données (LPD, RS 235.1). Cette règle vaut également lors des concentrations d'entreprises.

Lors des négociations, les entreprises proposent en règle générale aux acheteurs potentiels de procéder à une «vérification au préalable» (Due Diligence), afin qu'ils puissent étudier la situation économique de l'entreprise et évaluer sa valeur. Cette procédure permet aux personnes intéressées de se faire une idée des actifs de l'entreprise, mais aussi d'identifier les synergies possibles et les risques; elles peuvent ainsi évaluer les avantages que pourrait leur procurer un achat ou une fusion. Elles s'efforcent donc de recevoir le plus d'informations possible.

Une fois le contrat conclu, il est procédé à la fusion des entreprises ou à la reprise des parties d'entreprises. Les secteurs d'activité sont alors souvent réorganisés (voire regroupés) et des données personnelles transférées d'un secteur à l'autre, afin que l'entreprise restructurée puisse en profiter. Eu égard à la protection des données, il y aura lieu de veiller là aussi à ce que les données personnelles soient traitées dans le respect de la LPD.

Risques

Lors de la concentration d'entreprises, il existe deux risques principaux de violation de la protection des données: le traitement illicite et la transmission illicite de données. Lors de la phase de préparation et de conclusion du contrat, il peut arriver que l'entreprise transmette trop de données personnelles dans le cadre de la «vérification au préalable», et que les acheteurs potentiels obtiennent des informations (relatives à des personnes) dont ils n'ont pas besoin pour décider de racheter l'entreprise. Lors de la phase de reprise des entreprises ou des parties d'entreprises, le risque est de voir

des données personnelles transférées dans d'autres parties de l'entreprise ou être utilisées à une autre fin que celle indiquée lors de la collecte. Il est donc impératif, lors de fusions et de ventes d'entreprises, d'analyser les risques qui se posent en matière de protection des données et d'en tenir compte.

Risques lors de la phase de préparation et de conclusion du contrat

Dans le cadre de la procédure de «vérification au préalable», les entreprises déposent en règle générale toutes les informations utiles à l'évaluation de l'entreprise dans une salle d'information (Information Room), à laquelle les acheteurs potentiels ont accès; ceux-ci peuvent y consulter les différents documents et prendre des notes. Les informations mises à leur disposition concernent en général les fournisseurs, les clients, les collaborateurs et les autres partenaires de l'entreprise.

A ce stade, il existe deux risques principaux de transmission illicite de données:

- il peut arriver que des personnes se fassent passer pour des acheteurs potentiels alors qu'elles ne s'intéressent pas au rachat de l'entreprise mais uniquement aux informations fournies par cette dernière dans le cadre de la procédure de «vérification au préalable»;
- il peut arriver que l'entreprise (par inadvertance ou dans le but d'obtenir un montant plus élevé lors de la vente) rende disponibles des données personnelles qui ne sont pas nécessaires aux éventuels acheteurs.

Dans les deux cas, il peut y avoir violation de la protection des données. C'est pourquoi il importe que les entreprises soient sensibilisées à la question de la protection des données dès la phase de préparation du contrat.

Risques lors de la phase de reprise d'une entreprise

Lors de la concentration d'entreprises ou de la reprise d'une partie d'entreprise, certains secteurs sont restructurés ou regroupés, certaines tâches sont externalisées et les fichiers de données sont comparés et fusionnés. Une restructuration est souvent l'occasion pour les entreprises de procéder à une analyse en profondeur d'un secteur en vue d'améliorer son efficacité et sa rentabilité. Il arrive alors que des données personnelles soient transférées d'un secteur à l'autre et utilisées dans le nouveau secteur à des fins autres que celles indiquées aux personnes concernées lors de la collecte des données. Dans la plupart des cas, les entreprises n'agissent pas de mauvaise foi; le problème est en général simplement dû au fait que, suite à la restructuration, on a oublié dans quel but les données avaient été collectées.

Mesures et recommandations

Lors de concentrations d'entreprises, celles-ci sont tenues de respecter les principes applicables au traitement de données visés à l'art. 4 LPD. Si tel est le cas et qu'il existe en outre des motifs justificatifs au sens de l'art. 13 LPD, il est possible, dans le cadre d'une fusion, de traiter des données personnelles contre la volonté expresse de la personne concernée et de communiquer des données sensibles et des profils de la personnalité à des tiers. L'art. 13, al. 1, LPD prévoit comme motifs justificatifs le consentement de la victime, un intérêt prépondérant privé ou public ou une norme légale expresse. Plus concrètement, à l'al. 2, let. a, du même article, la loi mentionne par exemple expressément la conclusion ou l'exécution d'un contrat.

Dans les entreprises, il existe par ailleurs souvent des règles spécifiques prévoyant le secret professionnel ou un autre devoir de discrétion, règles dont le non-respect peut avoir des conséquences pénales. A cet égard, il convient de mentionner en particulier l'art. 35 LPD (Violation du devoir de discrétion) et l'art. 47 de la loi sur les banques (secret bancaire; LB, RS 952.0). Les règles prévoyant le secret de fonction doivent être respectées lors des concentrations d'entreprises.

S'agissant de la communication transfrontière de données personnelles, il convient de rappeler qu'aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées s'en trouve gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat (art. 6, al. 1, LPD).

Mesures à prendre lors de la phase de préparation et de conclusion du contrat

Au cours de la phase de préparation et de conclusion du contrat, la communication de données à des tiers dans le cadre de la procédure de «vérification au préalable» peut être admise en vertu de l'art. 13, al. 2, let. a, LPD, étant donné que l'acquéreur reprend l'intégralité des droits et obligations contractuels de l'entreprise acquise et devient par conséquent partie aux contrats que ladite entreprise a conclu avec ses clients. L'acquéreur doit dès lors garantir à ces clients qu'il s'acquittera de toutes les obligations contractuelles qui lui incombent suite au rachat de l'entreprise. Pour être en mesure d'évaluer les risques liés à ces obligations et déterminer s'il pourra tenir ces engagements, l'acheteur reçoit toutes les informations dont il a besoin dans le cadre de la procédure de «vérification au préalable». Dans ce contexte, il y a lieu de considérer que la transmission des données «est en relation directe avec (...) l'exécution d'un contrat» liant un client et la nouvelle entreprise (art. 13, al. 2, let. a, LPD). Cette règle s'applique tant aux données personnelles concernant les clients de l'entreprise qu'à celles relati-

ves aux collaborateurs. Toutefois, précisons que ces informations ne peuvent, en principe, pas être transmises à un acheteur potentiel avec référence nominale. Ce serait d'ailleurs contraire aux intérêts du vendeur: si les négociations échouent, l'acheteur potentiel pourrait alors être tenté de lui subtiliser ses collaborateurs et ses clients. Pour toutes ces raisons, il est indispensable que l'entreprise informe les personnes concernées avant toute transmission de données personnelles à des acheteurs (potentiels), afin qu'elles aient la possibilité de s'opposer à la transmission des données. Dans tous les cas, le vendeur devra veiller à ce que les acheteurs potentiels aient accès uniquement aux données personnelles dont ils ont réellement besoin.

Mesures à prendre lors de la phase de reprise d'une entreprise

Lors de la reprise d'une partie d'entreprise, il faut impérativement veiller à ce que les données personnelles transmises continuent d'être traitées dans le but indiqué lors de leur collecte, prévu par une loi ou ressortant des circonstances (art. 4, al. 2, LPD). Les entreprises ont donc l'obligation de garantir que seules les personnes autorisées auront accès aux données et que celles-ci seront toujours traitées dans le but prévu. C'est pourquoi il est indiqué de définir le but de chaque fichier de données interne et de préciser dans quel but et par qui les données peuvent être traitées, afin qu'il n'y ait pas de malentendu possible.

Recommandations

Phase de préparation et de conclusion du contrat

Lors des procédures de «vérification au préalable», le PFPDT recommande aux entreprises de prendre les mesures ci-après pour garantir aux personnes concernées une protection suffisante dans le domaine de la protection des données:

1. L'entreprise doit éviter de remettre des données personnelles à un acheteur potentiel ou à ses conseillers. Celui-ci doit tout au plus avoir la possibilité de consulter sur place les données qui lui sont utiles (dans un lieu aménagé à cet effet, le «Information Room»).
2. Lorsqu'une entreprise prévoit de mettre des informations à la disposition des acheteurs potentiels dans le «Information Room», elle devra veiller de manière rigoureuse à ce que seuls les acheteurs potentiels (et leurs conseillers) réellement intéressés par une reprise ou une fusion y ait accès.
3. Seul un cercle restreint de personnes doit avoir accès au «Information Room». Ces personnes devront en outre s'engager par contrat à ne pas réutiliser ces informations, voire à les détruire si les négociations n'aboutissent pas.

4. Les informations fournies devront toujours se limiter au strict nécessaire et à ce qui se justifie après pesée des intérêts, et être rendues anonymes dans la mesure du possible ou présentées de telle sorte qu'aucun lien ne puisse être établi avec des personnes données.

5. La quantité de données personnelles mises à la disposition des acheteurs potentiels pourra être adaptée à mesure que la procédure avance; elle pourra s'accroître si la conclusion du contrat paraît proche et le bouclement de l'affaire plus ou moins assuré.

6. En outre, il est indiqué, dans le cadre des procédures de «vérification au préalable», de conclure des accords de confidentialité (Non Disclosure Agreements, NDA) comprenant des clauses relatives à la protection des données, par lesquels les acheteurs potentiels et leurs conseillers s'engagent à garantir la protection des données. De tels accords constitueront un gage supplémentaire de sécurité, même s'il n'est pas possible d'exclure tout risque.

7. Les dispositions légales prévoyant l'obligation de garder le secret (cf. art. 35 LPD ou art. 47 LB, par ex.) doivent être respectées dans tous les cas.

Phase de reprise d'une entreprise

Lors de la phase de reprise d'une entreprise, le PFPDT recommande aux entreprises de prendre les mesures suivantes:

1. Avant d'utiliser les données de l'entreprise acquise, les responsables doivent examiner si le but indiqué lors de la collecte des données ou le but qui ressort des circonstances permettent de traiter les données dans le but prévu.

2. L'accès aux données des deux entreprises doit être réglé de telle sorte que, après la concentration, il soit accordé uniquement aux collaborateurs qui en ont réellement besoin.

3. En cas de doute (c.-à-d. dans le cas où il n'est pas possible de déterminer avec certitude si le droit permet de traiter les données dans le but prévu), il est indiqué d'informer les personnes en question du fait que des données les concernant feront l'objet d'un nouveau traitement dans le cadre de la fusion et, le cas échéant, de demander leur accord.

4. Les dispositions légales prévoyant l'obligation de garder le secret (cf. art. 35 LPD ou art. 47 LB, par ex.) doivent être respectées dans tous les cas.

4.1.5 Demande de décision concernant l'institution de prévoyance professionelle X

Voir chiffre 4.1.5 de la partie en langue allemande.

4.1.6 Recommandation concernant «Google Street View»

Voir chiffre 4.1.6 de la partie en langue allemande.

4.1.7 Recours concernant «Google Street View»

Voir chiffre 4.1.7 de la partie en langue allemande.

4.1.8 Recours concernant «KSS Schaffhausen»

Voir chiffre 4.1.8 de la partie en langue allemande.

4.1.9 Résolution concernant le renforcement de la coopération internationale en matière de protection des données et de la vie privée

31e Conférence internationale des commissaires à la protection des données et à la vie privée

Madrid, 4 – 6 novembre 2009

Résolution concernant le renforcement de la coopération internationale en matière de protection des données et de la vie privée

Le Préposé fédéral à la protection des données et à la transparence, Suisse

La Commission nationale de l'Informatique et des Libertés, France

La Commission de l'Informatique et des Libertés, Burkina Faso

La Commission d'accès à l'information, Québec (Canada)

Le Commissaire fédéral à la protection des données et au droit à l'information, Allemagne

L'Office de la protection des données, République Tchèque

Le Commissaire à la vie privée, Nouvelle-Zélande

Le Commissaire à la vie privée, Canada

L'Agence espagnole de la protection des données, Espagne

Résolution

La 31e Conférence Internationale des Commissaires à la Protection des données et à la vie privée

Rappelant:

(a) la résolution de la 31ème conférence sur les normes internationales sur la protection de la vie privée eu égard au traitement de données à caractère personnel

(b) la résolution de la 30e conférence sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles

(c) la résolution de la 30e conférence concernant la création d'un comité directeur relatif à la représentation lors de réunions des organismes internationaux

(d) la résolution de la 29e conférence internationale sur l'élaboration de normes internationales

(e) l'initiative de Londres présentée lors de la 28e Conférence

(f) la déclaration de Montreux adoptée lors de la 27e Conférence qui notamment appelle à la préparation d'un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée et par laquelle les commissaires convenaient de renforcer l'échange d'informations, la coordination de leurs activités de surveillance et le développement de standards communs

(g) la déclaration de Venise adoptée lors de la 22e Conférence

(h) la résolution de la 21ème conférence sur les règles d'accréditation des autorités de protection des données à la conférence internationale des commissaires à la protection des données qui fixe les conditions qu'une autorité de protection des données doit remplir pour être accréditée.

Prenant note que:

(a) la Conférence internationale des commissaires à la protection des données et à la vie privée se réunit chaque année depuis 31 ans et qu'elle constitue un forum toujours plus important pour la communauté internationale de la protection des données;

(b) le nombre d'autorités de protection des données accréditées auprès de la conférence est en constante augmentation et que ces nouvelles autorités contribuent au renforcement du caractère universel de la conférence;

(c) le travail accompli par le groupe de travail site Web en vue de la mise en place d'un site de la Conférence internationale afin notamment de favoriser la coopération et l'échange d'information entre les autorités accréditées constitue une étape importante en matière de coopération internationale.

Considérant que:

(a) la globalisation des traitements et des échanges de données à caractère personnel quel que soit le domaine d'activités et l'introduction des technologies de l'information et de la communication exigent une protection effective et universelle des droits et libertés fondamentales, notamment du droit à la protection des données et à la vie privée eu égard au traitement de données personnelles;

(b) le besoin croissant de coordonner les investigations et les interventions des autorités de protection des données nécessite un renforcement de la coopération internationale en matière de protection des données et de la vie privée, notamment avec la mise en place d'une organisation mondiale indépendante chargée de la protection des données et de la vie privée;

(c) la Conférence internationale pourrait ainsi jouer un rôle important dans la promotion et la mise en œuvre du droit à la protection des données et à la vie privée;

(d) il est nécessaire d'évaluer les besoins institutionnels de la Conférence internationale et de développer des options en vue de la création d'une structure plus formelle et le cas échéant d'en définir le mandat, les tâches et le financement.

Décide ce qui suit:

De créer un groupe de travail coordonné par les autorités organisant la 31e et la 32e Conférence internationale[1] et de lui confier les tâches suivantes:

(a) évaluer les besoins institutionnels de la Conférence internationale;

(b) développer des options en vue de la création d'un Secrétariat permanent comme structure plus formelle de la Conférence internationale; et

(c) soumettre un rapport à la 32e Conférence internationale avec des propositions concrètes.

[1] Le mandat pourrait être confié au groupe de contact mis en place par la résolution sur les normes internationales en matière de protection des données et de la vie privée soumise à l'approbation de la 31e Conférence internationale

4.2 Principe de la transparence

4.2.1 Recommandation adressée au Département fédéral de justice et police: «Conventions de résiliation des rapports de travail»

Berne, le 9 février 2009

Recommandation

émise au titre

de l'art. 14 de la loi fédérale du 17 décembre 2004
sur le principe de la transparence
dans l'administration

relativement à la demande en médiation introduite
par X
(demandeur)
contre
le Département fédéral de justice et police, Berne

I. Le Préposé fédéral à la protection des données et à la transparence constate ce qui suit:

1. Le demandeur, journaliste, a déposé par courrier daté du 5 février 2008 auprès du secrétariat général du Département fédéral de justice et police (DFJP) une demande d'accès selon la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans; RS 152.3) aux documents suivants:

- «le contrat de travail de Y, ancien secrétaire général du DFJP, en particulier les conditions spéciales qui lui ont été faites par l'ancien chef de département ainsi que la décision sur son indemnisation suite à son renvoi par la nouvelle cheffe du département.
- le contrat de travail de Z, ancien secrétaire général adjoint du DFJP, en particulier les conditions spéciales qui lui ont été faites par l'ancien chef de département ainsi que la décision sur son indemnisation suite à son renvoi par la nouvelle cheffe du département.»

D'après le sceau d'entrée du DFJP, la demande d'accès lui est parvenue le 6 mars 2008.

2. Le 17 mars 2008, le DFJP a refusé au demandeur l'accès au document conformément «aux art. 7 al. 2 et 9 LTrans, 6 de l'ordonnance sur la transparence (OTrans; RS 152.31), ainsi qu'à l'art. 19, al. 1 bis de la loi fédérale sur la protection des données (LPD; RS 235.1) et après une pesée des intérêts en présence […]». Concernant l'accès aux contrats de travail de Y et de Z, le DFJP a précisé que l'accès «[…] est également refusé en vertu de l'art. 23 LTrans, les documents en question étant manifestement antérieurs à l'entrée en vigueur de ladite loi (01.07.2006).»

3. Le demandeur a déposé une demande en médiation le 31 mars 2008 auprès du Préposé fédéral à la protection des données et à la transparence (préposé). Dans son courrier il a déclaré renoncer à demander «l'accès aux contrats de travail, puisque lesdits contrats ont manifestement été conclus avant l'entrée en vigueur de la LTrans et n'y sont pas soumis en vertu de l'art. 23 LTrans.» Par contre, le demandeur a maintenu sa demande en ce qui concerne «les décisions d'indemnisation des deux personnes susmentionnées au moment de leur départ du DFJP en raison des circonstances politiques qui ont entouré leur départ et le rôle très particulier qu'ils jouaient auprès de l'ancien chef du DFJP, M. Christoph Blocher.»

4. Sur demande du préposé, le DFJP a précisé dans sa prise de position du 15 mai 2008 ce qui suit: «Par ailleurs, le contrat de travail d'un employé de la Confédération, de même que les conventions de départ et que d'autres documents similaires, font partie du dossier personnel de l'employé qui, comme toutes les données personnelles relatives aux employés de l'administration fédérale, sont régies par l'Ordonnance concernant la protection des données person-

nelles (OPDP; RS 172.220.111.4)». Dès lors, «les dossiers du personnel ne sont accessibles qu'au service du personnel et aux responsables hiérarchiques» (art. 16, al. 2, OPDP) et «aucune donnée ne peut être communiquée à des tiers […] sans le consentement écrit de l'employé. […]» (art. 13, al. 1, OPDP). Le DFJP reconnaît toutefois «que la LTrans prime sur l'OPDP.» Le DFJP ajoute que l'identité des personnes en cause étant connue, les documents ne peuvent pas être anonymisés. Autoriser l'accès à ces documents équivaudrait donc à la communication de données personnelles au sens de l'art. 19, al. 1bis, de la loi fédérale sur la protection des données (LPD; RS 235.1). Conformément à cette disposition, les organes fédéraux peuvent communiquer des données personnelles dans le cadre de l'information officielle du public, d'office ou en vertu de la LTrans, aux conditions suivantes: (a.) les données concernées sont en rapport avec l'accomplissement de tâches publiques; (b.) la communication répond à un intérêt public prépondérant. En se référant aux art. 7, al. 2, LTrans et 6, al. 2, de l'ordonnance sur le principe de la transparence dans l'administration (ordonnance sur la transparence, OTrans; RS 152.31) le DFJP a émis l'opinion qu'aucun intérêt public prépondérant ne pouvait être invoqué en l'occurrence. Il avance l'argument «que les modalités de départ des deux collaborateurs […] n'ont jamais donné lieu à de grandes discussions dans le public, ni même au niveau politique, au contraire par exemple de la situation vécue lors du départ de [… l']ancien procureur général de la Confédération. En l'absence d'un quelconque événement important autre qu'une certaine curiosité journalistique, la seule fonction exercée par Y et Z ne suffit pas à justifier l'existence d'un besoin particulier d'informer le public sur les modalités de départ de ces derniers.»

Enfin le DFJP a souligné «que les conditions d'engagement et de départ des employés qualifiés (cadres) de la Confédération font l'objet de directives précises et impératives, toutes énoncées dans la Loi sur le personnel de la Confédération (LPers; RS 172.220.1) et ses diverses annexes. Une simple lecture de ces diverses dispositions légales suffisent (sic!) à (X) pour obtenir toutes les informations souhaitées, sans qu'il soit pour cela nécessaire de lui octroyer un accès au dossier personnel – et donc confidentiel – des deux collaborateurs visés dans sa demande.»

5. Conformément à l'art. 20 LTrans, le DFJP a transmis le 24 juin 2008 un dossier avec «l'ensemble de la correspondance, ainsi que les conventions de départ relatives aux personnes mentionnées».

6. Les contrats de travail de Y et de Z ont été conclus avant l'entrée en vigueur de la loi sur la transparence et ne sont donc pas accessibles (art. 23 LTrans). Le demandeur reconnaît explicitement ce fait dans sa demande en médiation.

   Le dossier transmis par le DFJP contient également en annexe les affaires du Conseil fédéral relatives au départ du secrétaire général et du secrétaire général suppléant, y compris les conventions de départ[1]. Conformément à l'art. 8, al. 1, LTrans, le droit d'accès n'est pas reconnu pour les documents officiels afférents à la procédure de co-rapport (à savoir les propositions et décisions du Conseil fédéral). Le préposé a déjà précisé dans une recommandation antérieure que les pièces jointes à une affaire du Conseil fédéral sont en principe soumises à la LTrans.[2]

   Il s'agit donc ci-après de juger si, en vertu de la loi sur la transparence, l'accès aux conventions de résiliation des rapports de travail passées entre la Confédération suisse et, respectivement, Y et Z doit être accordé ou non.

II. Le Préposé fédéral à la protection des données et à la transparence prend en considération les éléments suivants:

A. Médiation et recommandation selon l'art. 14 LTrans

161

1. En vertu de l'art. 13 LTrans, toute personne peut déposer une demande en médiation lorsque sa demande d'accès à des documents officiels est limitée, différée ou refusée, ou lorsque l'autorité n'a pas pris position sur sa demande dans les délais.

   Le préposé n'agit pas d'office, mais seulement sur la base d'une demande déposée par écrit.[3] Toute personne qui a pris part à une procédure de demande d'accès à des documents officiels est habilitée à introduire une demande en médiation. Pour la présentation de la demande en médiation, la forme écrite simple suffit. La demande doit spécifier que l'affaire est confiée au préposé. Elle doit être remise dans les 20 jours qui suivent la réception de la prise de position de l'autorité.

[1] Le Conseil fédéral est compétent pour conclure, modifier et résilier les rapports de travail des secrétaires généraux des départements et de leurs suppléants (art. 2, al. 1, let. d, de l'Ordonnance sur le personnel de la Confédération, RS 172.220.111.3)
[2] Recommandation du 30 juillet 2007: ODM / Liste des critères pour déterminer les pays sûrs (Safe Countries), ch. II.B.5 [en allemand]
[3] FF 2003 *1864*

2. Le demandeur a déposé une demande d'accès au sens de l'art. 6 LTrans auprès du DFJP et a reçu une réponse négative. Etant partie à la procédure de demande d'accès, il est légitimé à déposer une demande en médiation. Celle-ci a été remise au préposé en la forme (forme écrite simple) et dans les délais requis (20 jours à compter de la réception de la prise de position de l'autorité).

3. La procédure de médiation peut se dérouler par écrit ou de vive voix (en présence de tous les intéressés ou de certains d'entre eux), sous l'égide du préposé. C'est à lui qu'il incombe de fixer les modalités[4].

   Si la médiation n'aboutit pas ou si aucune solution consensuelle n'est envisageable, le préposé est tenu par l'art. 14 LTrans de formuler une recommandation fondée sur son appréciation de l'affaire.

B. Champ d'application matériel

1. Les conventions relatives à la résiliation des rapports de travail de Y et de Z font partie de leur *dossier personnel* et concernent leur sphère privée.

   Les dossiers personnels ne sont ni exclus globalement du champ d'application de la loi sur la transparence ni inclus dans la liste des exceptions au droit d'accès prévues à l'art. 7, al. 1, LTrans. Par conséquent, chaque demande d'accès à un document faisant partie d'un dossier personnel doit être jugée conformément aux dispositions de la loi sur la transparence.

   Dans la pratique, l'accès à un dossier personnel sera refusé dans la majorité des cas, au nom de la protection des données personnelles (art. 9 LTrans) et de la sphère privée (art. 7, al. 2, premier membre de la phrase, LTrans) des personnes concernées.

2. Au vu de ce qui précède, les dossiers personnels des employés de la Confédération ne sont en principe pas accessibles, du fait que la sphère privée des particuliers prime l'intérêt public à avoir accès à un document.[5]

[4] FF 2003 *1865*

[5] Cf. aussi Office fédéral de la justice, «Mise en œuvre du principe de la transparence au sein de l'administration fédérale: Questions fréquemment posées», 29.6.2006, ch. 3.3, et Recommandation du 23 décembre 2008: DFAE / Rapports sur l'inspection des visas, ch. II.B.2.ss. [en allemand]

3. Dans des *cas exceptionnels*, l'accès au dossier personnel complet (ou à un document qui en fait partie) peut être accordé, malgré le risque d'une atteinte à la sphère privée (art. 7, al. 2, second membre de la phrase, LTrans), et des données personnelles peuvent être communiquées à des tiers (art. 19, al. 1*bis*, LPD) – l'anonymisation d'un dossier personnel étant manifestement impossible. La condition *sine qua non* est toutefois que l'autorité en soit arrivée à la conclusion, après la pesée des intérêts en présence, que l'intérêt public à l'accès au document est prépondérant par rapport au droit d'un tiers à la protection de sa sphère privée. L'art. 6, al. 2, OTrans donne des points de repère pour tous les cas où un intérêt public prépondérant peut être invoqué à l'occasion de cette *pesée des intérêts dans un cas particulier*[6].

4. L'*intérêt public* peut être prépondérant lorsque le droit d'accès à un document répond à un besoin particulier d'information de la part du public (art. 6, al. 2, let. a, OTrans). Contrairement à l'avis du DFJP, le préposé est arrivé à la conclusion qu'il existe bel et bien un intérêt particulier pour le public à connaître la teneur des conditions d'engagement et de départ offertes dans *un cas concret* à un secrétaire général et à son suppléant (indépendamment du changement à la tête d'un département à la suite de la non-réélection d'un conseiller fédéral). En arguant que la consultation des dispositions légales pertinentes aboutirait au même résultat, le DFJP méconnaît le principe de la transparence, qui doit permettre aux citoyens de contrôler les décisions prises par l'administration. Le Conseil fédéral, dans son message relatif à la loi, fournit à ce sujet le commentaire suivant: «Le principe de transparence peut être considéré comme un instrument supplémentaire direct permettant de renforcer le contrôle direct de l'administration par les citoyens.»[7] C'est précisément en accordant l'accès aux conventions de départ discutées ici que la transparence peut être faite en ce qui concerne l'application correcte, même au plus haut niveau, des dispositions légales.

5. L'argument du DFJP, selon lequel les «modalités de départ des deux collaborateurs […] n'ont jamais donné lieu à de grandes discussions dans le public» et «qu'une certaine curiosité journalistique […] ne suffit pas à justifier l'existence d'un besoin particulier d'informer le public sur les modalités de départ de ces derniers», ne parvient pas à convaincre. D'une part, nous rappelons une fois de plus que l'exercice du droit d'accès ne présuppose en rien l'invocation

[6] Handkommentar BGÖ, Art. 7, RZ. 39ff. [cet ouvrage n'est disponible qu'en allemand]
[7] FF 2003 *1817*

d'un intérêt quelconque[8] (d'où il résulte que la simple curiosité suffit); d'autre part, la teneur de l'ordonnance n'exige aucunement que l'intérêt particulier à être informé soit obligatoirement lié à des événements importants, ces derniers n'y figurant qu'à titre d'exemple («notamment»). De plus, la résiliation des rapports de travail de Y et de Z s'inscrit dans le contexte de la non-réélection du chef du département d'alors et de l'élection d'une nouvelle cheffe du département par le Parlement, événements qui ont indubitablement donné lieu à de grandes discussions.

6. Différents critères peuvent être mis en œuvre pour évaluer la gravité de l'*atteinte à la sphère privée* dans un cas concret.

   Il faut tenir compte, d'une part, de la nature des données en question et des conséquences qu'entraînerait leur publication. Le contenu des deux documents à évaluer ici s'aligne sur les directives légales applicables au départ d'un secrétaire général ou d'un secrétaire général suppléant; on n'y trouve donc aucune donnée personnelle spécifique ou «sensible» concernant Y ou Z. L'octroi de l'accès aux conventions de départ n'entraîne donc qu'une atteinte peu importante, voire nulle, à la sphère privée de Y et de Z. D'autre part, il faut tenir compte de la fonction ou du poste occupés par la personne concernée par l'octroi de l'accès. Dans la mesure où les informations personnelles sont en relation directe avec la fonction officielle exercée, les personnes concernées doivent s'accommoder d'atteintes plus étendues à leur sphère privée que le personnel administratif subordonné[9]. Cette condition est remplie en l'occurrence, étant donné que Y et Z sont respectivement concernés à titre de secrétaire général et de secrétaire général suppléant, les deux fonctions les plus élevées dans la hiérarchie départementale après le chef du département.

7. En résumé nos conclusions sont les suivantes:

   - le droit d'accès aux conventions réglant la résiliation des rapports de travail de Y et de Z répond à un besoin particulier d'information du public (art. 6, al. 2, let. a, OTrans);

[8] FF 2003 *1843*; Handkommentar BGÖ, Art. 6, RZ. 22

[9] «Ordonnance relative à la loi sur la transparence. Commentaire», du 24.5.2006, ch. 3.5; Brunner «Öffentlichkeit der Verwaltung und informationelle Selbstbestimmung: Von Kollisionen und Verkehrsregeln», ch. IV 3; dans «Selbstbestimmung und Recht», Festgabe für Rainer J. Schweizer, Schulthess 2003

- Y et Z n'ont à subir qu'une atteinte limitée à leur sphère privée du fait de l'octroi de l'accès aux conventions réglant la résiliation de leurs rapports de travail;
- l'intérêt public à l'accès aux conventions réglant la résiliation des rapports de travail de Y et de Z l'emporte sur l'intérêt qu'ont les deux personnes concernées à préserver leur sphère privée.

8. Se fondant sur les considérations ci-dessus, le préposé conclut que l'accès aux conventions relatives à la résiliation des rapports de travail de Y et de Z doit être accordé.

9. Droit d'être entendu:

   Le préposé communique la présente recommandation à Y et à Z, reconnus comme tiers au sens de l'art. 7, al. 2, LTrans. Ils ont ainsi – de même que le demandeur – la possibilité d'exiger du DFJP qu'il leur notifie une décision contre laquelle ils pourront recourir auprès du Tribunal administratif fédéral.

III. Se fondant sur les considérations ci-dessus, le Préposé fédéral à la protection des données et à la transparence recommande ce qui suit:

1. Le Département fédéral de justice et police accorde l'accès aux documents intitulés «Vereinbarung betreffend die Auflösung des Arbeitsverhältnisses im gegenseitigen Einvernehmen», passés Y et avec Z, conformément à l'art. 7, al. 2, de la loi sur la transparence, en relation avec l'art. 6, al. 2, de l'ordonnance sur la transparence.

2. Le Département fédéral de justice et police rend une décision selon l'art. 5 de la loi sur la procédure administrative, s'il refuse d'octroyer l'accès conformément à la recommandation (chiffre III.1.).

   Le Département fédéral de justice et police rend la décision dans les vingt jours qui suivent la réception de la recommandation (art. 15, al. 3, LTrans).

3. Dans les dix jours qui suivent la réception de la recommandation, le demandeur et les tiers concernés par la présente recommandation (Y et Z) peuvent demander que le Département fédéral de justice et police (DFJP) rende une

décision selon l'art. 5 de la loi fédérale sur la procédure administrative (art. 15, al. 1, LTrans), s'ils ne sont d'accord avec la recommandation (chiffre III.1).

4. La décision peut faire l'objet d'un recours devant le Tribunal administratif fédéral (art. 16 LTrans).

5. La présente recommandation est publiée (art. 13, al. 3, de l'ordonnance sur la transparence, OTrans; RS 152.31). Afin de protéger les données relatives aux parties et aux personnes concernées à la procédure de médiation, le nom du demandeur a été anonymisé.

6. La recommandation est notifiée:

   - à X

   - au Département fédéral de justice et police
     Secrétariat général
     3003 Berne

   - à Y

   - à Z

Hanspeter Thür

4.2.2 Recommandation adressée à l'Office fédéral des migrations: «Données brutes de SYMIC»

Voir chiffre 4.2.2 de la partie en langue allemande.

4.2.3 Recommandation adressée à l'Administration fédérale des contributions: «Cockpits/Amtsreportings»

Voir chiffre 4.2.3 de la partie en langue allemande.

4.2.4 Recommandation adressée au Département fédéral de l'environnement, des transports, de l'énergie et de la communication: «Documentation complémentaire relative au compte d'État» (I)

Voir chiffre 4.2.4 de la partie en langue allemande.

4.2.5 Recommandation adressée aux sécretariats des Départements: (DFI, DFJP, DDPS, DFF, DFE,DETEC): «Documentation complémentaire relative au compte d'État» (II)

Voir chiffre 4.2.5 de la partie en langue allemande.